Instalar y configurar vCenter Server

Actualización 3
9 de febrero de 2022
VMware vSphere 7.0
vCenter Server 7.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de la instalación y la configuración de vCenter Server

Instalar y configurar vCenter Server describe cómo se implementa el dispositivo VMware vCenter Server®.

En VMware, valoramos la inclusión. Para fomentar este principio dentro de nuestra comunidad de clientes, socios y personal interno, creamos contenido con un lenguaje inclusivo.

Audiencia prevista

Instalar y configurar vCenter Server es para cualquier persona que deba instalar y configurar VMware vSphere®. Estos temas están destinados a administradores de sistemas Microsoft Windows o Linux experimentados que estén familiarizados con las operaciones de los centros de datos y la tecnología de máquinas virtuales.

Introducción a la instalación y configuración de vSphere

1

vSphere 7.0 proporciona diferentes opciones para la instalación y configuración. Para garantizar una implementación correcta de vSphere, debe comprender las opciones de instalación y configuración y la secuencia de tareas.

Los dos componentes principales de vSphere son ESXi y vCenter Server. ESXi es la plataforma de virtualización en la cual puede crear y ejecutar máquinas virtuales y aplicaciones virtuales. vCenter Server es un servicio que actúa como administrador central para hosts de ESXi conectados en una red. vCenter Server permite agrupar y administrar los recursos de varios hosts.

Debe implementar vCenter Server Appliance, una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server y los componentes de vCenter Server. Puede implementar la instancia de vCenter Server Appliance en hosts ESXi o instancias de vCenter Server.

Para obtener información detallada sobre el proceso de instalación de ESXi, consulte *Instalar y configurar VMware ESXi*.

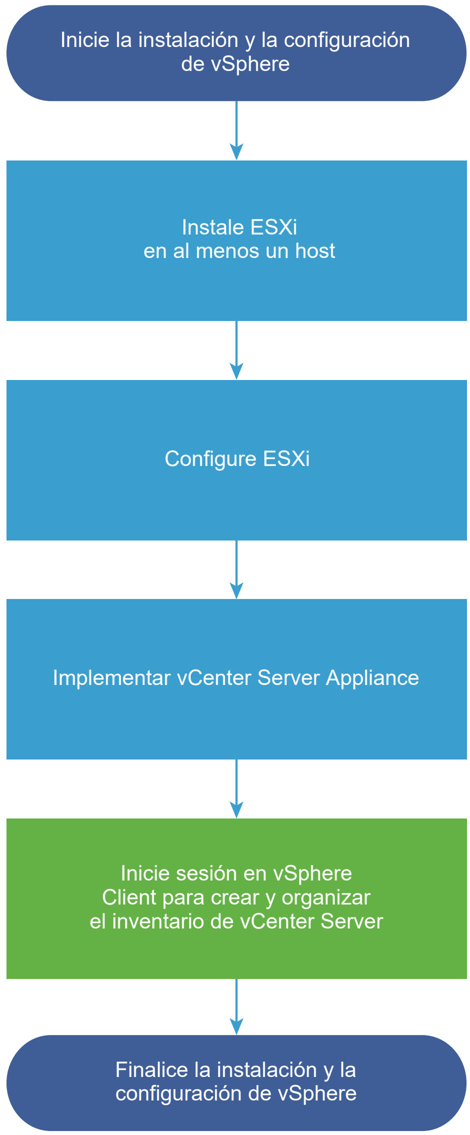
Este capítulo incluye los siguientes temas:

Información general del proceso de instalación y configuración de vSphere

vSphere es un producto sofisticado con varios componentes que puede instalar y configurar. A fin de garantizar una implementación correcta de vSphere, comprenda la secuencia de las tareas requeridas.

La instalación de vSphere incluye las siguientes tareas:

Figura 1-1. Flujo de trabajo de instalación y configuración de vSphere



1 Lea las notas de la versión de vSphere.

2 Instale ESXi.

Nota Consulte *Instalar y configurar VMware ESXi* para obtener información detallada sobre el proceso de instalación de ESXi.

3 Ajuste la configuración de red y arranque de ESXi, la consola directa y otras opciones. Para obtener más información, consulte *Instalar y configurar VMware ESXi*.

4 Considere la posibilidad de configurar un servidor de Syslog para inicio de sesión remoto, a fin de garantizar que haya almacenamiento en disco suficiente para los archivos de registro. La configuración del registro en un host remoto es especialmente importante para hosts con almacenamiento local limitado. Consulte *Instalar y configurar VMware ESXi*.

5 Instale vCenter Server.

   Puede implementar la instancia de vCenter Server Appliance en un host ESXi o una instancia de vCenter Server.

   Puede implementar o instalar varias instancias de vCenter Server conectadas mediante una configuración de Enhanced Linked Mode; para ello, regístrelas en un dominio común de Single Sign-On.

   a Consulte los temas en Requisitos de sistema para la vCenter Server Appliance y compruebe que el sistema cumpla con los requisitos de hardware y software para la implementación del dispositivo.

   b Determine el método de implementación que desea utilizar.

      Puede utilizar el método de GUI para implementar de manera interactiva el dispositivo. De manera alternativa, puede utilizar el método de CLI para realizar una implementación silenciosa del dispositivo. Consulte Implementar la GUI de vCenter Server Appliance y Implementar la CLI de vCenter Server Appliance.

   c Utilice el tema Información requerida para implementar una instancia de vCenter Server Appliance para crear una hoja de trabajo con la información necesaria para la implementación de GUI, o utilice el tema Preparar el archivo de configuración JSON para la implementación de CLI a fin de crear las plantillas JSON para la implementación de CLI.

   d Implemente el dispositivo.

6 Conéctese a vCenter Server desde vSphere Client. Consulte Capítulo 5 Después de implementar vCenter Server Appliance.

7 Configure la instancia de vCenter Server. Consulte *Configuración de vCenter Server* y *Administrar vCenter Server y hosts*.

Componentes y servicios de vCenter Server

vCenter Server proporciona una plataforma centralizada para la administración, el funcionamiento, el aprovisionamiento de recursos y la evaluación del rendimiento de las máquinas virtuales y los hosts.

Cuando se implementa vCenter Server Appliance, vCenter Server, los componentes de vCenter Server y los servicios de autenticación se implementan en el mismo sistema.

Los siguientes componentes se incluyen en las implementaciones de vCenter Server Appliance:

- Los servicios de autenticación contienen vCenter Single Sign-On, License Service, Lookup Service y VMware Certificate Authority.
- El grupo de servicios de vCenter Server contiene vCenter Server, vSphere Client, vSphere Auto Deploy y vSphere ESXi Dump Collector. La instancia de vCenter Server Appliance también contiene el servicio de extensión de VMware vSphere Lifecycle Manager y VMware vCenter Lifecycle Manager.

Qué ocurrido con Platform Services Controller

A partir de vSphere 7.0, la implementación de una nueva instancia de vCenter Server o la actualización a vCenter Server 7.0 requiere el uso de vCenter Server Appliance, una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server. La nueva instancia de vCenter Server contiene todos los servicios de Platform Services Controller y conserva la funcionalidad y los flujos de trabajo, incluidos la autenticación, la administración de certificados, las etiquetas y la concesión de licencias. Ya no es necesario ni es posible implementar y utilizar una instancia de Platform Services Controller externa. Todos los servicios de Platform Services Controller se consolidan en vCenter Server, y se simplifican la implementación y la administración.

Dado que estos servicios ahora forman parte de vCenter Server, ya no se describen como parte de Platform Services Controller. En vSphere 7.0, la publicación de *vSphere Authentication* reemplaza la publicación de *Administrar Platform Services Controller*. La nueva publicación contiene información completa sobre la autenticación y la administración de certificados. Para obtener información sobre la actualización o la migración de las implementaciones de vSphere 6.5 y 6.7 con una instancia externa existente de Platform Services Controller a vSphere 7.0 mediante vCenter Server Appliance, consulte la documentación de *Actualizar vSphere*.

Servicios de autenticación

vCenter Single Sign-On

El servicio de autenticación de vCenter Single Sign-On proporciona servicios de autenticación segura a los componentes de software de vSphere. Mediante el uso de vCenter Single Sign-On, los componentes de vSphere se comunican entre sí a través de un mecanismo de intercambio de token seguro, en lugar de requerir que cada componente autentique a un usuario por separado con un servicio de directorio como Active Directory. vCenter Single Sign-On utiliza vsphere.local como el dominio en el que se registran las soluciones y los componentes de vSphere durante el proceso de instalación o actualización, lo que proporciona un recurso de infraestructura. vCenter Single Sign-On puede autenticar a usuarios de sus propios usuarios y grupos internos, o bien, puede conectarse a servicios de directorio externos de confianza, como Microsoft Active Directory. A continuación, los usuarios autenticados pueden recibir asignaciones de permisos o roles registrados y basados en soluciones dentro de un entorno de vSphere.

Se requiere vCenter Single Sign-On con vCenter Server.

License Service de vSphere

License Service de vSphere proporciona capacidades comunes de inventario y administración de licencias a todos los sistemas de vCenter Server en el dominio de Single Sign-On.

VMware Certificate Authority

VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado que tiene VMCA como la entidad de certificación raíz de forma predeterminada. El aprovisionamiento ocurre cuando el host ESXi se agrega a vCenter Server de forma explícita

o como parte del proceso de instalación del host ESXi. Todos los certificados de ESXi se almacenan localmente en el host.

Para obtener información sobre todas las capacidades y los servicios de autenticación, consulte *vSphere Authentication*.

Servicios instalados con vCenter Server

Estos componentes adicionales se instalan de forma silenciosa cuando se instala vCenter Server. Los componentes no pueden instalarse por separado, puesto que no poseen sus propios instaladores.

PostgreSQL

Una versión integrada de la distribución de VMware de la base de datos de PostgreSQL para vSphere y vCloud Hybrid Services.

vSphere Client

La interfaz de usuario basada en HTML5 que permite conectarse a instancias de vCenter Server por medio de un explorador web. Este vSphere Client reemplaza el vSphere Web Client basado en Flex en vSphere 7.0.

vSphere ESXi Dump Collector

Herramienta de soporte de vCenter Server. Puede configurar ESXi para guardar la memoria VMkernel en un servidor de red, en lugar de un disco, cuando el sistema detecta un error crítico. vSphere ESXi Dump Collector recopila los volcados de memoria en la red.

vSphere Auto Deploy

La herramienta de soporte de vCenter Server que puede aprovisionar cientos de hosts físicos con software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. O bien, puede especificar perfiles de host para aplicar a los hosts y una ubicación de vCenter Server (carpeta o clúster) para cada host.

Extensión de VMware vSphere Lifecycle Manager

vSphere Lifecycle Manager permite la administración centralizada y automatizada de revisiones y versiones para VMware vSphere y ofrece soporte para hosts ESXi, máquinas virtuales y dispositivos virtuales VMware. La extensión de VMware vSphere Lifecycle Manager es un servicio opcional de vCenter Server Appliance.

VMware vCenter Lifecycle Manager

vCenter Lifecycle Manager automatiza el proceso de las máquinas virtuales y las quita de servicio en el momento adecuado. vCenter Lifecycle Manager coloca automáticamente los servidores en función de su ubicación, organización, entorno, nivel de servicio o niveles de rendimiento. Cuando se encuentra una solución para un conjunto de criterios, la máquina se implementa automáticamente.

Descripción de vCenter Server Appliance

vCenter Server Appliance es una máquina virtual preconfigurada que está optimizada para ejecutar vCenter Server y los servicios asociados.

El paquete de vCenter Server Appliance contiene el siguiente software:

- Photon OS® 3.0
- Los servicios de autenticación de vSphere
- PostgreSQL
- Extensión de VMware vSphere Lifecycle Manager
- VMware vCenter Lifecycle Manager

La versión 7.0 de vCenter Server se implementa con la versión 10 del hardware virtual, que admite 64 CPU virtuales por máquina virtual en ESXi.

Durante la implementación, puede seleccionar el tamaño de vCenter Server Appliance para el tamaño del entorno de vSphere y el tamaño de almacenamiento para los requisitos de base de datos.

vCenter Server usa el servicio de extensión de VMware vSphere Lifecycle Manager. Ya no se requiere una instancia externa de vSphere Lifecycle Manager en Windows para la administración automatizada y centralizada de revisiones y versiones de vSphere. Para obtener más información sobre vCenter Server, consulte Componentes y servicios de vCenter Server.

vCenter Server es compatible con la alta disponibilidad. Para obtener más información sobre la configuración de vCenter Server en un clúster de vCenter de alta disponibilidad, consulte *Disponibilidad de vSphere*.

vCenter Server es compatible con la copia de seguridad y la restauración basada en archivos. Para obtener información sobre las operaciones de copia de seguridad y restauración, consulte Capítulo 3 Restaurar vCenter Server y crear una copia de seguridad de ella con base en archivos.

Para obtener información sobre los máximos de vCenter Server, consulte Máximos de configuración de VMware.

Información sobre los dominios de vSphere y los nombres de dominio

Cada instancia de vCenter Server está asociada con un dominio de vCenter Single Sign-On. El valor predeterminado del nombre de dominio es vsphere.local, pero puede cambiarlo durante la implementación. El dominio determina el espacio de autenticación local.

Dominio de vCenter Single Sign-On

Cuando implemente una instancia de vCenter Server Appliance, se le solicitará que cree un dominio de vCenter Single Sign-On o que se una a un dominio existente.

VMware Directory Service (vmdir) usa el nombre del dominio para todas las estructuras internas del Protocolo Simplificado de Acceso a Directorios (LDAP).

Puede asignarle a su dominio un nombre único. Para evitar conflictos de autenticación, use un nombre que OpenLDAP, Microsoft Active Directory y otros servicios de directorio no usen.

Después de especificar el nombre para el dominio, puede agregar usuarios y grupos. Puede agregar un origen de identidad de Active Directory o LDAP, y permitir a los usuarios y grupos de dicho origen que se autentiquen. También puede agregar al dominio instancias de vCenter Server, o bien otros productos VMware, como vRealize Operations.

vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode permite iniciar sesión en cualquier instancia única de vCenter Server, además de ver y administrar los inventarios de todos los sistemas vCenter Server del grupo.

Puede unirse a un máximo de 15 implementaciones de vCenter Server Appliance con vCenter Enhanced Linked Mode en un único dominio de vSphere Single Sign-On.

Puede crear un grupo de vCenter Enhanced Linked Mode durante la implementación de vCenter Server Appliance.

También puede unirse a un grupo de vCenter Enhanced Linked Mode moviendo o redireccionando una instancia de vCenter Server de un dominio de vSphere a otro dominio existente. Consulte Redireccionar una instancia de vCenter Server a otra instancia de vCenter Server en un dominio diferente para obtener información sobre el redireccionamiento de un nodo de vCenter Server.

vCenter Enhanced Linked Mode para vCenter Server Appliance

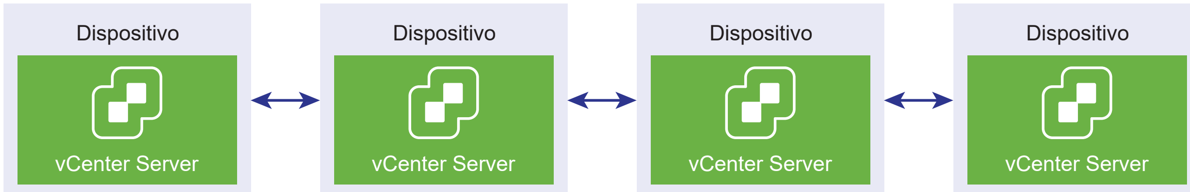
Se habilitó la compatibilidad con Enhanced Linked Mode para implementaciones de vCenter Server Appliance.

Puede conectar las implementaciones de vCenter Server Appliance para formar un dominio.

Entre estas funciones se encuentran las siguientes:

- El proceso de copia de seguridad y restauración es simple. Consulte Capítulo 3 Restaurar vCenter Server y crear una copia de seguridad de ella con base en archivos para obtener más información.
- El proceso de HA es simple, ya que no se necesitan equilibradores de carga.
- Es posible vincular hasta 15 implementaciones de vCenter Server Appliance mediante Enhanced Linked Mode y mostrarlas en una sola vista de inventario.
- Para un clúster de vCenter High Availability (vCenter HA), tres nodos se consideran un nodo lógico de vCenter Server. Consulte "Descripción general de la arquitectura de vCenter" en *Disponibilidad de vSphere* para obtener un resumen de la arquitectura de vCenter HA. Un clúster de vCenter HA necesita una única licencia estándar de vCenter Server.

Figura 1-2. Enhanced Linked Mode para implementaciones de vCenter Server Appliance



Enhanced Linked Mode con replicación de solo lectura

Si una instancia de vCenter High Availability (vCenter HA) está conectada a otra instancia de vCenter Server que tiene habilitado Enhanced Linked Mode, y se produce conmutación por error de vCenter HA en el nodo pasivo y no puede comunicarse con su socio de replicación en el otro nodo de vCenter Server, la réplica en el nodo de vCenter HA entra en modo de solo lectura.

Unirse a un dominio de vCenter Enhanced Linked Mode

Puede unir una instancia de vCenter Server Appliance a otro nodo durante la implementación de la instancia de vCenter Server Appliance.

Nota También puede unirse a un grupo de vCenter Enhanced Linked Mode moviendo o redireccionando una instancia de vCenter Server de un dominio de vSphere a otro dominio existente. Consulte Redireccionar una instancia de vCenter Server a otra instancia de vCenter Server en un dominio diferente para obtener información sobre el redireccionamiento de un nodo de vCenter Server.

Por ejemplo, puede implementar dos sistemas vCenter Server Appliance y unir los dos nodos con vCenter Enhanced Linked Mode.

Si implementa los nodos de vCenter Server Appliance con el instalador de interfaz de usuario:

1 Para el dispositivo 1, implemente la instancia de vCenter Server Appliance como una instancia en el host ESXi 1. Sincronice la configuración de hora con el host ESXi 1.

2 Para el dispositivo 2, implemente la instancia de vCenter Server Appliance como una instancia en el host ESXi 1 y ajuste la configuración de hora para que el dispositivo 2 se sincronice con el host ESXi 1. En la etapa 2, seleccione unir el servidor vCenter Single Sign-On del dispositivo implementado en el dispositivo 1. Para obtener instrucciones específicas, consulte Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Si implementa los nodos de vCenter Server Appliance con la CLI:

1 Establezca los parámetros de la plantilla de configuración JSON `embedded_vCSA_on_VC.json` (o `embedded_vCSA_on_ESXi.json`) para el dispositivo 1 como una instancia en el host ESXi 1. Consulte Preparar el archivo de configuración JSON para la implementación de CLI para obtener instrucciones específicas sobre la preparación del archivo de configuración JSON.

2 Implemente el dispositivo 1 mediante el comando `vcsa-cli-installer`. Consulte Implementar vCenter Server Appliance mediante la CLI para obtener instrucciones.

3 Establezca los parámetros de la plantilla de configuración JSON `embedded_vCSA_replication_on_VC.json` (o `embedded_vCSA_replication_on_ESXi.json`) para el dispositivo 2 como una instancia en el host ESXi 1. Introduzca el nombre de host del primer nodo integrado en el campo `replication_partner_hostname` de la sección `sso`.

4 Implemente el dispositivo 2 mediante el comando `vcsa-cli-installer` utilizando el archivo `embedded_vCSA_replication_on_VC.json` (o `embedded_vCSA_replication_on_ESXi.json`).

Implementar vCenter Server Appliance

2

vCenter Server Appliance se puede implementar para administrar un entorno de vSphere.

Es posible implementar vCenter Server Appliance en un host ESXi 6.5 o posterior, o en un host ESXi o un clúster de DRS desde el inventario de una instancia de vCenter Server 6.5 o posterior.

Para obtener información sobre el software que se incluye en vCenter Server Appliance 7.0, consulte Descripción de vCenter Server Appliance.

Para obtener información sobre los requisitos de software y hardware para implementar vCenter Server Appliance, consulte Requisitos de sistema para la vCenter Server Appliance.

El instalador de vCenter Server contiene archivos ejecutables para implementaciones de GUI y CLI.

- La implementación de GUI es un proceso de dos etapas. En la primera etapa, un asistente de implementación implementa el archivo OVA para el dispositivo en el host ESXi o la instancia de vCenter Server de destino. Una vez completada la implementación de OVA, el usuario es redirigido a la segunda etapa del proceso en la que se instalan y se inician los servicios del dispositivo recién implementado.
- El método de implementación de CLI implica ejecutar un comando de CLI en un archivo JSON preparado previamente. El instalador de CLI analiza los parámetros de configuración y los valores indicados en el archivo JSON, y genera un comando de OVF Tool para implementar y configurar automáticamente el dispositivo. La implementación de la CLI ejecuta automáticamente la etapa 1 y luego la etapa 2, sin necesidad de interacción del usuario.

vCenter Server Appliance tiene los siguientes nombres de usuario predeterminados:

Nombre de usuario	Descripción
root	Utilice este nombre de usuario para iniciar sesión en el sistema operativo del dispositivo y la interfaz de administración de vCenter Server. La contraseña se establece durante la implementación del dispositivo virtual.
administrator@*su_nombre_de_dominio*	Utilice este nombre de usuario para iniciar sesión en vCenter Single Sign-On. La contraseña se establece durante la creación del dominio de vCenter Single Sign-On. El dominio de vCenter Single Sign-On se crea durante la implementación de una instancia de vCenter Server Appliance en un dominio de vCenter Single Sign-On nuevo. Después de que se cree un dominio de vCenter Single Sign-On, solo el usuario administrator@*su_nombre_de_dominio* contará con los privilegios necesarios para iniciar sesión en vCenter Single Sign-On y vCenter Server. El usuario administrator@*su_nombre_de_dominio* puede proceder de la siguiente manera: ■ Agregar un origen de identidad en el cual los usuarios y grupos tienen definido vCenter Single Sign-On. ■ Otorgar permisos a los usuarios y grupos. Para obtener información sobre cómo agregar orígenes de identidad y conceder permisos a usuarios y grupos, consulte *vSphere Authentication*.

Para obtener información sobre la actualización y la aplicación de revisiones de vCenter Server Appliance, consulte *Actualizar vSphere*.

Para obtener información sobre la configuración de vCenter Server, consulte *Configuración de vCenter Server*.

Si desea configurar vCenter Server para usar una versión de dirección IPv6, utilice el nombre de dominio completo (FQDN) o el nombre de host del dispositivo. Para configurar una dirección IPv4, la práctica recomendada es usar el FQDN o nombre de host del dispositivo, ya que la dirección IP puede cambiar si se asigna mediante DHCP.

Este capítulo incluye los siguientes temas:

- Requisitos de sistema para la vCenter Server Appliance
- Prepararse para implementar vCenter Server Appliance
- Requisitos previos para implementar vCenter Server Appliance
- Implementar la GUI de vCenter Server Appliance
- Implementar la CLI de vCenter Server Appliance

Requisitos de sistema para la vCenter Server Appliance

Puede implementar la instancia de vCenter Server Appliance en un host ESXi 6.5 o una versión posterior, o en una instancia de vCenter Server 6.5 o una versión posterior. El sistema también debe cumplir con los requisitos específicos de software y hardware.

Al usar nombres de dominios completos, asegúrese de que el equipo cliente que use para implementar el dispositivo y la red en la que implementa el dispositivo utilicen el mismo servidor DNS.

Antes de implementar el dispositivo, sincronice los relojes del servidor de destino y todas las instancias de vCenter Server de la red de vSphere. Los relojes sin sincronizar pueden ocasionar problemas de autenticación y pueden producir un error en la instalación o impedir que se inicien los servicios del dispositivo. Consulte Sincronizar los relojes en la red de vSphere.

Requisitos de hardware para el dispositivo de vCenter Server

Cuando implemente vCenter Server Appliance, puede seleccionar implementar un dispositivo que sea adecuado para el tamaño del entorno de vSphere. La opción que seleccione determina la cantidad de CPU y la cantidad de memoria para el dispositivo.

Requisitos de hardware para el dispositivo de vCenter Server

Los requisitos de hardware para vCenter Server Appliance dependen del tamaño del inventario de vSphere.

Tabla 2-1. Requisitos de hardware para la instancia de vCenter Server Appliance

	Cantidad de vCPU	Memoria
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	2	12 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	4	19 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	8	28 GB
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	16	37 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	24	56 GB

Nota Si desea agregar un host ESXi con más de 512 LUN y 2048 rutas de acceso al inventario de vCenter Server, debe implementar vCenter Server Appliance para un entorno grande o extragrande.

Requisitos de almacenamiento para el dispositivo de vCenter Server

Al implementar la instancia de vCenter Server Appliance, el host ESXi o el clúster de DRS en el que se implementa el dispositivo debe cumplir con requisitos mínimos de almacenamiento. El almacenamiento necesario depende no solo del tamaño del entorno de vSphere y del tamaño del almacenamiento, sino también del modo de aprovisionamiento del disco.

Requisitos de almacenamiento para el dispositivo de vCenter Server

Los requisitos de almacenamiento son diferentes para cada tamaño de entorno de vSphere y dependen de los requisitos de tamaño de la base de datos.

Tabla 2-2. Requisitos de almacenamiento para una instancia de vCenter Server Appliance

	Tamaño de almacenamiento predeterminado	Tamaño de almacenamiento grande	Tamaño de almacenamiento extragrande
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	579 GB	1992 GB	4279 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	694 GB	2046 GB	4304 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	908 GB	2140 GB	4468 GB
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	1358 GB	1958 GB	4518 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	2283 GB	2383 GB	4620 GB

Nota Los requisitos de almacenamiento incluyen los requisitos de la instancia de vSphere Lifecycle Manager que se ejecuta como servicio en la instancia de vCenter Server Appliance.

Requisitos de software para vCenter Server Appliance

VMware vCenter Server Appliance se puede implementar en hosts ESXi 6.5 o posteriores, o bien en instancias de vCenter Server 6.5 o posteriores.

vCenter Server Appliance se puede implementar mediante el instalador de GUI o CLI. Se ejecuta el instalador de un equipo cliente en red que se utiliza para conectarse al servidor de destino e implementar el dispositivo en el servidor. Puede conectarse directamente a un host ESXi 6.5 en el que implementar el dispositivo. Igualmente, puede conectarse a una instancia de vCenter Server 6.5 para implementar el dispositivo en un host ESXi o un clúster de DRS que residen en el inventario de vCenter Server.

Para obtener información sobre los requisitos del equipo cliente en red, consulte Requisitos del sistema para el instalador de vCenter Server.

Puertos necesarios en vCenter Server

El sistema vCenter Server debe poder enviar datos a cada host administrado y recibir datos de vSphere Client. Para permitir las actividades de migración y aprovisionamiento entre los hosts

administrados, los hosts de origen y destino deben poder recibir datos entre sí a través de los puertos TCP y UDP predeterminados.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios. Para obtener la lista de todos los puertos y protocolos compatibles en vSphere, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com.

Durante la instalación, si un puerto se encuentra en uso o está bloqueado mediante una lista de no permitidos, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación. Hay puertos internos que se utilizan solo para la comunicación entre los procesos.

VMware utiliza los puertos designados para la comunicación. Además, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si existe un firewall integrado entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Client, consulte la documentación de *Administrar vCenter Server y hosts*.

Requisitos de DNS para vCenter Server Appliance

Al implementar vCenter Server Appliance, de manera similar a cualquier servidor de red, es posible asignar una dirección IP fija y un FQDN que se pueda resolver mediante un servidor DNS, de modo que los clientes puedan acceder al servicio con confianza.

La implementación de vCenter Server Appliance con una dirección IP estática permite garantizar que la dirección IP del dispositivo siga siendo la misma en caso de que el sistema se reinicie.

Antes de implementar vCenter Server Appliance con una dirección IP estática, debe verificar que esta dirección IP tenga un registro de sistema de nombres de dominio (Domain Name System, DNS) interno válido.

Cuando se implementa vCenter Server Appliance, la instalación del componente de servidor web que admite la instancia de vSphere Client genera un error si el instalador no puede buscar el nombre de dominio completo (FQDN) del dispositivo desde su dirección IP. La búsqueda inversa se implementa mediante registros PTR.

Si planea usar un FQDN para el nombre de sistema del dispositivo, debe comprobar que el FQDN pueda resolverse mediante un servidor DNS agregando registros DNS A de avance y retroceso.

Se puede utilizar el comando `nslookup` para comprobar que el servicio de búsqueda inversa de DNS devuelva un FQDN cuando se realice una consulta con la dirección IP y que el FQDN pueda resolverse.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

Si utiliza DHCP en lugar de una dirección IP estática para vCenter Server Appliance, compruebe que el nombre de dispositivo se actualice en el servicio de nombres de dominio (Domain Name Service, DNS). Si puede hacer ping al nombre del dispositivo; el nombre se actualiza en DNS.

Asegúrese de que la interfaz de administración del host ESXi tenga una resolución de DNS válida desde vCenter Server y todas las instancias de vSphere Client. Asegúrese de que vCenter Server tenga una resolución de DNS válida desde todos los hosts ESXi y las instancias de vSphere Client.

Requisitos de software de vSphere Client

El uso de vSphere Client requiere un explorador web compatible.

VMware ha probado y admite los siguientes sistemas operativos invitados y versiones de explorador para vSphere Client.

Sistemas operativos invitados compatibles

- Windows de 32 bits y 64 bits
- Mac OS

Versiones de exploradores compatibles

- Google Chrome 89 o posterior
- Mozilla Firefox 80 o posterior
- Microsoft Edge 90 o posterior

Nota Es posible que las versiones posteriores de estos exploradores funcionen, pero no se han probado.

Prepararse para implementar vCenter Server Appliance

Antes de implementar vCenter Server Appliance, debe descargar el archivo ISO de instalación de vCenter Server y montarlo en una máquina virtual de red o en un servidor físico desde donde desea realizar la implementación.

El equipo desde el cual implementa el dispositivo se debe ejecutar en un sistema operativo Windows, Linux o Mac que cumpla con los requisitos del sistema operativo. Consulte Requisitos del sistema para el instalador de vCenter Server.

Requisitos del sistema para el instalador de vCenter Server

Puede ejecutar el instalador de GUI o CLI de vCenter Server desde un equipo cliente de red que se ejecuta en una versión compatible de un sistema operativo Windows, Linux o Mac.

Para garantizar el rendimiento óptimo de los instaladores de GUI y CLI, use un equipo cliente que cumpla con los requisitos mínimos de hardware.

Tabla 2-3. Requisitos del sistema para los instaladores de GUI y CLI

Sistema operativo	Versiones compatibles	Configuración de hardware mínima para un rendimiento óptimo
Windows	■ Windows 8, 8.1, 10 ■ Windows 2012 de 64 bits ■ Windows 2012 R2 de 64 bits ■ Windows 2016 de 64 bits ■ Windows 2019 x64	4 GB de RAM, 2 CPU con 4 núcleos con 2,3 GHz, disco duro de 32 GB, 1 NIC
Linux	■ SUSE 15 ■ Ubuntu 16.04 y 18.04	4 GB de RAM, 1 CPU con 2 núcleos con 2,3 GHz, disco duro de 16 GB, 1 NIC **Nota** El instalador de CLI requiere un sistema operativo de 64 bits.
Mac	■ macOS v10.13, 10.14, 10.15 ■ macOS High Sierra, Mojave, Catalina	8 GB de RAM, 1 CPU con 4 núcleos con 2,4 GHz, disco duro de 150 GB, 1 NIC

Nota Para los equipos cliente que se ejecutan en Mac 10.13 o una versión posterior, no se admiten las implementaciones de GUI simultáneas de varios dispositivos. Debe implementar los dispositivos en una secuencia.

Nota Deben instalarse las bibliotecas redistribuibles de Visual C++ para ejecutar el instalador de CLI en las versiones de Windows anteriores a Windows 10. Los instaladores de Microsoft de estas bibliotecas se encuentran en el directorio `vcsa-cli-installer/win32/vcredist`.

Nota La implementación de vCenter Server Appliance con la GUI requiere una resolución mínima de 1.024 x 768 para verse correctamente. Las resoluciones más bajas pueden truncar los elementos de interfaz de usuario.

Descargar el instalador de vCenter Server y montarlo

VMware lanzó la imagen ISO de vCenter Server Appliance, donde se incluyen los instaladores de GUI y CLI para vCenter Server Appliance.

Con los archivos ejecutables de GUI y CLI que se incluyen en el instalador de vCenter Server, es posible:

- implementar vCenter Server Appliance;

- actualizar vCenter Server appliance;
- converger las versiones anteriores de vCenter Server con una instancia externa de Platform Services Controller a la versión actual de vCenter Server;
- restaurar una instancia de vCenter Server Appliance a partir de una copia de seguridad basada en archivos.

Requisitos previos

- Cree una cuenta de Customer Connect en https://my.vmware.com/web/vmware/.
- Compruebe que el equipo cliente cumpla con los requisitos del sistema para el instalador de vCenter Server. Consulte Requisitos del sistema para el instalador de vCenter Server.

Procedimiento

1 Inicie sesión en VMware Customer Connect.

2 Desplácese hasta **Productos y cuentas > Todos los productos**.

3 Busque VMware vSphere y haga clic en **Ver componentes de descarga**.

4 Seleccione una versión de VMware vSphere en el menú desplegable **Seleccionar versión**.

5 Seleccione una versión de VMware vCenter Server y haga clic en **IR A DESCARGAS**.

6 Descargue la imagen ISO de vCenter Server Appliance.

7 Confirme que md5sum sea correcto mediante una herramienta de suma de comprobación MD5.

8 Monte la imagen ISO en el equipo cliente desde el cual desea implementar, actualizar, migrar o restaurar el dispositivo.

Nota No se admite software de montaje de ISO en el que no se permitan más de ocho niveles de directorio, por ejemplo, MagicISO Maker en Windows.

No se admite Archive Manager en los sistemas operativos Linux y Mac.

Se puede usar DiskImageMounter en el sistema operativo Mac.
Se puede usar Disk Image Mounter en Ubuntu 14.04.
Se puede usar el terminal en el sistema operativo SUSE 12.

```
$ sudo mkdir mount_dir
$ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
```

Importante Debido a un cambio de seguridad en MacOS Catalina, debe modificar la configuración de seguridad en su equipo hasta que se complete la implementación de vCenter Server. Si intenta ejecutar el instalador en MacOS Catalina sin modificar la configuración de seguridad, el instalador de vCenter Server muestra el error:`ovftool cannot be opened because the developer cannot be verified`. Para obtener más información, consulte el artículo 79416 de la base de conocimientos.

Pasos siguientes

Abra el archivo `readme.txt` y revise la información sobre los otros archivos y directorios en la imagen ISO de vCenter Server Appliance.

Sincronizar los relojes en la red de vSphere

Compruebe que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes en las máquinas físicas de la red de vSphere no están sincronizados, los certificados SSL y los tokens SAML, que están sujetos a limitaciones temporales, pueden no reconocerse como válidos en las comunicaciones entre máquinas de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar errores en la instalación o evitar que se inicie el servicio `vmware-vpxd` de vCenter Server.

Las incoherencias de hora en vSphere pueden provocar un error en el primer arranque de los diferentes servicios según la ubicación en el entorno donde la hora no sea precisa y el momento en el que se sincronice la hora. Normalmente, los problemas se producen cuando el host ESXi de destino para la instancia de vCenter Server de destino no está sincronizado con NTP o PTP. De forma similar, se pueden presentar problemas si el dispositivo vCenter Server de destino se migra a un host ESXi establecido en otra hora debido a un DRS completamente automatizado.

Para evitar problemas de sincronización de hora, asegúrese de que lo siguiente sea correcto antes de instalar, migrar o actualizar un dispositivo vCenter Server.

- El host ESXi de destino donde se desea implementar la instancia de vCenter Server de destino está sincronizado con NTP o PTP.
- El host ESXi donde se ejecuta la instancia de vCenter Server de origen está sincronizado con NTP o PTP.
- Al actualizar o migrar desde vSphere 6.5 o 6.7 a vSphere 7.0, si la instancia de vCenter Server Appliance está conectada a una instancia externa de Platform Services Controller, asegúrese de que el host ESXi donde se ejecuta la instancia externa de Platform Services Controller esté sincronizado con NTP o PTP.
- Si va a actualizar o migrar de vSphere 6.5 o 6.7 a vSphere 7.0, compruebe que la instancia de origen de vCenter Server Appliance y la instancia externa de vCenter Server y el Platform Services Controller tengan la hora correcta.
- Cuando se actualiza una instancia de vCenter Server 6.5 o 6.7 con una instancia externa de Platform Services Controller a vSphere 7.0, el proceso de actualización se convierte en una instancia de vCenter Server con Platform Services Controller integrado.

Verifique que todos los equipos host de Windows en los que se ejecuta vCenter Server estén sincronizados con el servidor de tiempo de red (NTP). Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1318.

Para sincronizar los relojes de ESXi con un servidor NTP o un servidor PTP, puede usar VMware Host Client. Para obtener información sobre cómo editar la configuración de hora de un host ESXi, consulte *Administrar un host único de vSphere: VMware Host Client*.

Para obtener información sobre cómo cambiar la configuración de sincronización de hora para vCenter Server, consulte "Configurar la zona horaria y la sincronización de hora del sistema" en *Configuración de vCenter Server*.

Para obtener información sobre cómo editar la configuración de hora de un host mediante vSphere Client, consulte "Editar la configuración de hora para un host" en *Administrar vCenter Server y hosts*.

Sincronización del reloj del sistema entre el cliente y el servidor

Para establecer una conexión segura de TLS con una instancia de vCenter Server (el servidor), el sistema donde se ejecuta el instalador de CLI (el cliente) no debe tener un reloj del sistema que sea más lento o más rápido que el reloj del sistema del servidor dentro de un límite aceptable (tolerancia).

Consulte en Tabla 2-4. Tolerancia de reloj de cliente los valores específicos para cada escenario de implementación.

Nota Los valores de reloj de cliente solo se aplican en vCenter Server 6.7 y versiones posteriores.

Tabla 2-4. Tolerancia de reloj de cliente

Escenario de implementación	Tolerancia de reloj	Notas de la conexión
Vincular una instancia de vCenter Server con otra instancia de vCenter Server	Al implementar la segunda instancia de vCenter Server, la tolerancia de reloj del cliente y de la primera instancia de vCenter Server no debe superar los 10 minutos.	
Instalar vCenter Server Appliance con una instancia de vCenter Server de contenedor con una plantilla `*._on_vc.json`.	La tolerancia de reloj máxima entre el cliente y la instancia contenedora de vCenter Server es de 8 horas y 20 minutos.	

Requisitos previos para implementar vCenter Server Appliance

Para garantizar una correcta implementación de vCenter Server Appliance, es necesario realizar algunas tareas y comprobaciones previas obligatorias antes de ejecutar el instalador.

Requisitos previos generales

- Descargar el instalador de vCenter Server y montarlo.

Requisitos previos de sistema de destino

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte Requisitos de sistema para la vCenter Server Appliance.
- Si desea implementar el dispositivo en un host ESXi, compruebe que el host ESXi no esté en modo de bloqueo o de mantenimiento y que no forme parte de un clúster de DRS completamente automatizado.
- Si planea implementar el dispositivo en un clúster de DRS en el inventario de una instancia de vCenter Server, compruebe que el clúster contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento.
- Si desea utilizar servidores NTP para la sincronización de hora, compruebe que los servidores NTP estén en ejecución, y que la hora de esos servidores esté sincronizada con la del servidor de destino en el que desea implementar el dispositivo.

Requisitos previos de vCenter Enhanced Linked Mode

Al implementar una nueva instancia de vCenter Server como parte de una implementación de Enhanced Linked Mode, cree una copia de seguridad basada en imágenes de los nodos de vCenter Server existentes en el entorno. Puede utilizar la copia de seguridad como precaución en caso de que se produzca un error durante el proceso de implementación.

Si se produce un error en la implementación, elimine la instancia de vCenter Server Appliance recién implementada y restaure los nodos de vCenter Server a partir de sus respectivas copias de seguridad basadas en imágenes. Debe restaurar todos los nodos del entorno a partir de las copias de seguridad basadas en imágenes. Si no lo hace, es posible que los socios de replicación no estén sincronizados con el nodo restaurado.

- Para obtener más información sobre cómo crear implementaciones de vCenter Enhanced Linked Mode, consulte vCenter Enhanced Linked Mode.
- Para obtener información sobre las copias de seguridad basadas en imágenes, consulte Capítulo 4 Restaurar y crear copias de seguridad con base en imágenes de un entorno de vCenter Server.

Requisitos previos de red

Si desea asignar una dirección IP estática y un FQDN como nombre del sistema en la configuración de red del dispositivo, compruebe que se hayan configurado los registros de DNS inversos y directos para la dirección IP.

Implementar la GUI de vCenter Server Appliance

El instalador de la GUI se puede utilizar para realizar una implementación interactiva de una instancia de vCenter Server Appliance.

Al realizar la implementación de la GUI, debe descargar el instalador de vCenter Server en un equipo cliente de red, ejecutar el asistente de implementación desde el equipo cliente y proporcionar las entradas requeridas para implementar y configurar el dispositivo.

El proceso de implementación de la GUI incluye una serie de dos etapas.

Figura 2-1. Etapa 1: Implementación de OVA



En la primera etapa, se utiliza el asistente de implementación para elegir el tipo de implementación y la configuración del dispositivo. En esta etapa, se completa la implementación del archivo OVA en el servidor de destino con el tipo de implementación y la configuración del dispositivo que se proporciona.

Como alternativa a realizar la primera etapa de la implementación con el instalador de GUI, puede implementar el archivo OVA de vCenter Server Appliance mediante el uso de vSphere Client. Después de la implementación de OVA, debe iniciar sesión en la interfaz de administración de vCenter Server del dispositivo que se acaba de implementar para seguir con la segunda etapa del proceso de implementación. Consulte "Implementar una plantilla de OVF o de OVA" en *Administrar máquinas virtuales de vSphere* Administrar máquinas virtuales de vSphere para obtener información sobre la implementación de un archivo OVA mediante vSphere Client.

Figura 2-2. Etapa 2: Configuración del dispositivo



En la segunda etapa, se utiliza el asistente de configuración para configurar la sincronización de hora del dispositivo y vCenter Single Sign-On. En esta etapa, finaliza la configuración inicial y se inician los servicios del dispositivo recientemente implementado.

Como alternativa a la segunda etapa de la implementación con el instalador de GUI, puede iniciar sesión en la interfaz de administración de vCenter Server del dispositivo que se acaba de implementar, https://*FQDN_or_IP_address*:5480.

Información requerida para implementar una instancia de vCenter Server Appliance

Cuando se utiliza el método de GUI para implementar una instancia de vCenter Server Appliance, el asistente solicita información de implementación y configuración. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de trabajo a fin de registrar la información necesaria para implementar una instancia de vCenter Server Appliance.

Tabla 2-5. Información requerida durante la etapa 1 del proceso de implementación de GUI

Información necesaria	Predeterminado	Su entrada
El FQDN o la dirección IP del servidor de destino donde se desea implementar el dispositivo. El servidor de destino puede ser un host ESXi o una instancia de vCenter Server.	-	
Puerto HTTPS del servidor de destino	443	
Nombre de usuario con privilegios administrativos en el servidor de destino ■ Si el servidor de destino es un host ESXi, use el nombre de usuario raíz. ■ Si el servidor de destino es una instancia de vCenter Server, use *nombre_de_usuario@nombre_de_dominio*, por ejemplo, administrator@vsphere.local.	-	
Contraseña del usuario con privilegios administrativos en el servidor de destino	-	
Centro de datos del inventario de vCenter Server donde se desea implementar el dispositivo. El servidor de destino debe ser una instancia de vCenter Server. De manera opcional, puede proporcionar una carpeta para el centro de datos.	-	
Host ESXi o clúster de DRS del inventario del centro de datos donde se desea implementar el dispositivo	-	
Nombre de la máquina virtual para el dispositivo ■ No debe contener signos de porcentaje (%), barras diagonales inversas (\) ni barras diagonales (/). ■ No debe tener más de 80 caracteres.	vCenter Server	
Contraseña del usuario raíz del sistema operativo del dispositivo ■ Debe contener únicamente caracteres ASCII inferiores, sin espacios. ■ Debe contener al menos 8 caracteres y no más de 20. ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!).	-	

Tabla 2-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Información necesaria	Predeterminado	Su entrada
Tamaño de implementación de la instancia de vCenter Server Appliance para el entorno de vSphere. Consulte Requisitos de hardware para el dispositivo de vCenter Server para obtener información sobre los tamaños de implementación que puede seleccionar. La opción que seleccione determina la cantidad de CPU y la cantidad de memoria para el dispositivo.	Muy pequeño	
Tamaño de almacenamiento de la instancia de vCenter Server Appliance para el entorno de vSphere. El almacenamiento requerido depende no solo del tamaño del entorno de vSphere, sino también del modo de aprovisionamiento del disco. Consulte Requisitos de almacenamiento para el dispositivo de vCenter Server. Incremente el tamaño de almacenamiento predeterminado si desea un volumen mayor para datos SEAT (estadísticas, eventos, alarmas y tareas).	Predeterminado	
Nombre del almacén de datos donde se desean almacenar los archivos de configuración y los discos virtuales del dispositivo **Nota** El instalador muestra una lista de almacenes de datos a los que se puede acceder desde el servidor de destino.	-	
Habilitar o deshabilitar el modo de disco fino	Deshabilitado	
Nombre de la red a la que se conectará el dispositivo **Nota** El instalador muestra un menú desplegable con redes que dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable. Debe poder accederse a la red desde el equipo cliente donde se realiza la implementación.	-	
Versión IP de la dirección del dispositivo Puede ser IPv4 o IPv6.	IPv4	
Asignación de direcciones IP de la dirección del dispositivo Puede ser estática o DHCP.	estático	

Tabla 2-5. Información requerida durante la etapa 1 del proceso de implementación de GUI (continuación)

Información necesaria	Predeterminado	Su entrada
FQDN Para una asignaciones de IP estática vCenter Server utiliza el FQDN o la dirección IP como nombre del sistema.	-	
Dirección IP	-	
Para redes IPv4, puede utilizar una máscara de subred o un prefijo de red. La máscara de subred utiliza una notación de decimal con punto (por ejemplo, 255.255.255.0). Un prefijo de red IPv4 es un número entero entre 0 y 32. Para redes IPv6, debe utilizar un prefijo de red. Un prefijo de red IPv6 es un número entero entre 0 y 128.	-	
Puerta de enlace predeterminada	-	
Servidores DNS separados por comas	-	
Nombre del sistema (FQDN) Solo si utiliza DHCP con IPv4 y tiene un servidor DNS dinámico (DDNS) disponible en su entorno.	-	

Tabla 2-6. Información requerida durante la etapa 2 del proceso de implementación de GUI

Información necesaria	Predeterminado	Su entrada
Configuración de sincronización de hora Puede sincronizar la hora del dispositivo con la hora del host ESXi o con uno o varios servidores NTP. Si desea usar más de un servidor NTP, debe proporcionar las direcciones IP o FQDN de los servidores NTP como lista separada por comas.	Sincronizar la hora con los servidores NTP	
Habilitar o deshabilitar el acceso SSH **Nota** vCenter Server High Availability requiere acceso SSH remoto al dispositivo.	Deshabilitado	
Nombre del nuevo dominio de vCenter Single Sign-On Por ejemplo, vsphere.local.	-	

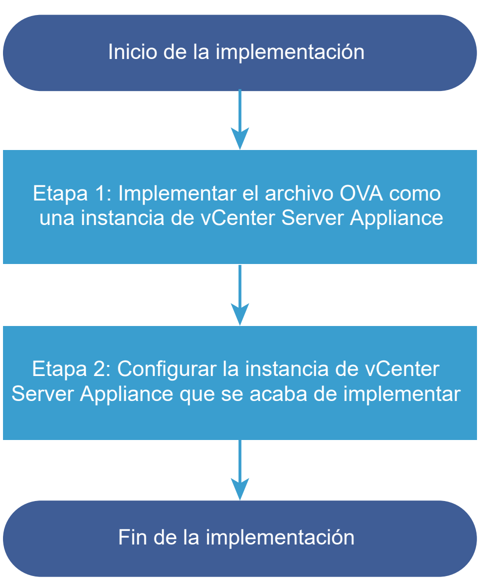
Tabla 2-6. Información requerida durante la etapa 2 del proceso de implementación de GUI (continuación)

Información necesaria	Predeterminado	Su entrada
Contraseña de la cuenta de administrador, administrator@*nombre_del_dominio*. ■ Debe contener al menos 8 caracteres y no más de 20. ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%)	-	
Contraseña del usuario administrador de vCenter Single Sign On para el dominio	-	
Decida si desea unirse al Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.	Unirse al CEIP	

Implementar vCenter Server Appliance mediante la GUI

El instalador de la GUI se puede utilizar para realizar una implementación interactiva de una instancia de vCenter Server Appliance. Se debe ejecutar la implementación de GUI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Figura 2-3. Flujo de trabajo de implementación de un dispositivo de vCenter Server



Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance.
- Consulte Información requerida para implementar una instancia de vCenter Server Appliance.

Procedimiento

1 Etapa 1: Implementar el archivo OVA como dispositivo de vCenter Server

   En la etapa 1 del proceso de implementación, se implementa el archivo OVA, que está incluido en el instalador de vCenter Server como dispositivo de vCenter Server.

2 Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado

   Cuando la implementación de OVA termina, se le redirige a la etapa 2 del proceso de implementación para que configure e inicie los servicios de la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Etapa 1: Implementar el archivo OVA como dispositivo de vCenter Server

En la etapa 1 del proceso de implementación, se implementa el archivo OVA, que está incluido en el instalador de vCenter Server como dispositivo de vCenter Server.

Procedimiento

1 En el instalador de vCenter Server, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.

   - En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
   - En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
   - En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.

2 En la página de inicio, haga clic en **Instalar** para iniciar el asistente de implementación.

3 Revise la página de introducción para comprender el proceso de implementación y haga clic en **Siguiente**.

4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.

5 Conéctese al servidor de destino donde desea implementar vCenter Server Appliance.

Opción	Pasos
Puede conectarse a un host ESXi para implementar el dispositivo allí.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar un host ESXi o un clúster de DRS donde se implementará el dispositivo.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*su_nombre_de_dominio*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contiene el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

6 En la página Configurar máquina virtual de dispositivo, escriba un nombre para el dispositivo de vCenter Server, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

El nombre del dispositivo no debe contener ningún signo de porcentaje (%), ninguna barra inversa (\) ni ninguna barra diagonal (/), y tampoco debe tener más de 80 caracteres.

La contraseña debe contener solo caracteres ASCII inferiores sin espacios, al menos ocho caracteres, un número, letras minúsculas y mayúsculas, y un carácter especial, por ejemplo, un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

7 Seleccione el tamaño de implementación de la instancia de vCenter Server Appliance para el inventario de vSphere.

Consulte Requisitos de hardware para el dispositivo de vCenter Server para obtener información sobre los tamaños de implementación que puede seleccionar. La opción que seleccione determina la cantidad de CPU y la cantidad de memoria para el dispositivo.

8 Seleccione el tamaño de almacenamiento de la instancia de vCenter Server Appliance y haga clic en **Siguiente**.

El almacenamiento requerido depende no solo del tamaño del entorno de vSphere, sino también del modo de aprovisionamiento del disco. Consulte Requisitos de almacenamiento para el dispositivo de vCenter Server.

9 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar modo de disco fino** para habilitar el aprovisionamiento fino. Los almacenes de datos NFS utilizan aprovisionamiento fino de forma predeterminada.

10 En la página Ajustar la configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Red	Seleccione la red a la que desea conectar el dispositivo. Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.
Versión IP	Seleccione la versión de la dirección IP del dispositivo. Puede seleccionar la versión IPv4 o IPv6.
Asignación de IP	Seleccione cómo asignar la dirección IP del dispositivo. ■ **estático** El asistente solicita que se introduzca la dirección IP y la configuración de red. ■ **DHCP** Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno. Si hay un DDNS habilitado en el entorno, puede escribir el nombre de dominio completo (Fully Qualified Domain Name, FQDN) que prefiera para el dispositivo.
Puertos comunes	Puede personalizar los puertos HTTP y HTTPS (opcionales). Si desea especificar un número de puerto HTTP y HTTPS personalizado, asegúrese de no usar un número de puerto que ya se use en vCenter Server ni los puertos HTTP y HTTPS 80 y 443 predeterminados.

11 En la página Listo para finalizar la etapa 1, revise la configuración de implementación del dispositivo de vCenter Server y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

12 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de implementación a fin de configurar e iniciar los servicios del dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración de vCenter Server para configurar e iniciar los servicios.

Resultados

El dispositivo de vCenter Server recién implementado está en ejecución en el servidor de destino, pero no se inician los servicios.

Etapa 2 - Configure la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado

Cuando la implementación de OVA termina, se le redirige a la etapa 2 del proceso de implementación para que configure e inicie los servicios de la instancia de vCenter Server Appliance recién implementada con Platform Services Controller integrado.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de implementación y haga clic en **Siguiente**.

2 Ajuste la configuración de la hora en el dispositivo. De manera opcional, habilite el acceso SSH remoto al dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Sincronizar la hora con los servidores NTP	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, deberá escribir los nombres o las direcciones IP de los servidores NTP separados por comas.

3 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	Crea un nuevo dominio de vCenter Single Sign-On. a Introduzca el nombre de dominio; por ejemplo, `vsphere.local`. **Nota** Asegúrese de que el nombre de dominio no contenga letras mayúsculas. b Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. Esta es la contraseña del usuario administrator@*su_nombre_de_dominio*. c Confirme la contraseña del administrador y haga clic en **Siguiente**.
Unirse a un dominio de vCenter Single Sign-On existente	Se une a un nuevo servidor vCenter Single Sign-On en un dominio de vCenter Single Sign-On existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On. a Escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor vCenter Single Sign-On al que se va a unir. b Introduzca el puerto HTTPS que se usará para la comunicación con el servidor vCenter Single Sign-On. c Escriba el nombre de dominio de vCenter Single Sign-On al que desee unirse; por ejemplo, `vsphere.local`. d Escriba la contraseña de la cuenta de administrador de vCenter Single Sign-On. e Haga clic en **Siguiente**.

Si decide unirse a un dominio de vCenter Single Sign-On existente, se habilita la característica Enhanced Linked Mode. Los datos de la infraestructura se replican con el servidor vCenter Single Sign-On unido.

4 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

5 En la página Listo para finalizar, revise los ajustes de configuración del dispositivo de vCenter Server, haga clic en **Finalizar** y en **Aceptar** para completar la etapa 2 del proceso de implementación y configurar el dispositivo.

6 (opcional) Cuando finalice la configuración inicial, introduzca la dirección URL del explorador con **https://*vcenter_server_appliance_fqdn*/ui**, desplácese hasta vSphere Client e inicie sesión en la instancia de vCenter Server de vCenter Server Appliance, o haga clic en **https://*vcenter_server_appliance_fqdn*:443** para ir a la página Introducción de vCenter Server Appliance.

7 Haga clic en **Cerrar** para cerrar el asistente.

Se le redirigirá a la página Introducción de vCenter Server Appliance.

Pasos siguientes

Es posible configurar la alta disponibilidad para vCenter Server Appliance. Para obtener información sobre la forma de proporcionar alta disponibilidad a vCenter Server Appliance, consulte *Disponibilidad de vSphere*.

Implementar la CLI de vCenter Server Appliance

Puede utilizar el instalador de CLI para realizar la implementación silenciosa de vCenter Server Appliance en un host ESXio una instancia de vCenter Server.

El proceso de implementación de CLI incluye: descargar el instalador de vCenter Server en la máquina virtual de red o en el servidor físico desde donde se desea realizar la implementación; preparar un archivo de configuración JSON con la información de implementación; y ejecutar el comando de implementación.

También puede ver el vídeo sobre cómo instalar el dispositivo de vCenter Server mediante el instalador de CLI.

(Instalación con línea de comandos de vCenter Server)

Preparar el archivo de configuración JSON para la implementación de CLI

Antes de ejecutar el instalador de CLI para implementar una instancia de vCenter Server Appliance, debe preparar un archivo JSON con los parámetros de configuración y sus valores para la especificación de la implementación.

El instalador de vCenter Server contiene plantillas JSON para todas las opciones de implementación. Para obtener información sobre las plantillas, consulte Plantillas JSON para la implementación de CLI de vCenter Server Appliance.

Para implementar un dispositivo con la configuración mínima, establezca los valores según los parámetros de configuración en la plantilla JSON correspondiente a su especificación. Puede editar los valores preestablecidos, quitar los parámetros de configuración y agregar parámetros para configuraciones personalizadas.

Si desea conocer la lista completa de parámetros de configuración y sus descripciones, desplácese hasta el subdirectorio del instalador del sistema operativo y ejecute el comando `vcsa-deploy install --template-help`, o bien consulte Parámetros de configuración de implementación.

Requisitos previos

- Debe estar familiarizado con la sintaxis JSON.
- Descargar el instalador de vCenter Server y montarlo.

Procedimiento

1 En el instalador de vCenter Server, desplácese hasta el directorio `vcsa-cli-installer` y abra la subcarpeta `plantillas`.

2 Copie las plantillas de implementación desde la subcarpeta `install` en su área de trabajo.

Importante La ruta de acceso a los archivos de configuración JSON debe contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

3 En un editor de texto, abra el archivo de plantilla de la especificación.

Para garantizar la correcta sintaxis del archivo de configuración JSON, use un editor JSON.

4 Complete los valores para los parámetros de configuración requeridos y, como opción, introduzca parámetros adicionales y sus valores.

Por ejemplo, si desea utilizar una asignación de DHCP IPv4 para la red del dispositivo, en la subsección `network` de la plantilla, cambie el valor del parámetro `mode` a `dhcp` y quite los parámetros de configuración predeterminados que son para una asignación estática.

```
        "network": {
            "ip_family": "ipv4",
            "mode": "dhcp"
        },
```

Importante Los valores de cadena, incluidas las contraseñas, deben contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

Para establecer un valor que contiene una barra diagonal inversa (\) o un carácter de comillas ("), debe anteponer a este carácter una barra diagonal inversa (\). Por ejemplo, `"password":"my\"password"` establece la contraseña my"password y `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-7.0.0.`*`XXXX-YYYYYYY`*`_OVF10.ova"` establece la ruta de acceso `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.`*`XXXX-YYYYYYY`*`_OVF10.ova`.

Los valores booleanos deben contener únicamente caracteres en minúsculas; es decir, un valor puede ser `true` o `false`. Por ejemplo, `"ssh_enable":false`.

5 (opcional) Para validar un archivo JSON, utilice un editor JSON de su elección.

6 Guárdelo en formato UTF-8 y cierre el archivo.

Pasos siguientes

Puede crear y guardar plantillas adicionales, si fuera necesario, para la especificación de la implementación.

Plantillas JSON para la implementación de CLI de vCenter Server Appliance

El instalador de vCenter Server incluye plantillas JSON con los parámetros de configuración mínimos para todas las opciones de implementación. Las plantillas están ubicadas en el directorio `vcsa-cli-installer/templates/install`.

Por cada opción de implementación, hay una plantilla que permite implementar el dispositivo en un host ESXi y otra plantilla que permite implementar el dispositivo en una instancia de vCenter Server.

Tabla 2-7. Las plantillas de implementación JSON se incluyen en el instalador de vCenter Server.

Plantilla	Descripción
`embedded_vCSA_on_ESXi.json`	Contiene los parámetros de configuración mínimos que se necesitan para la implementación de vCenter Server Appliance en un host ESXi.
`vCSA_with_cluster_on_ESXi.json`	Contiene los parámetros de configuración mínimos que se necesitan para la implementación de vCenter Server Appliance junto con un clúster de vSAN de un solo nodo y un clúster administrado por vLCM en un host ESXi.
`embedded_vCSA_on_VC.json`	Contiene los parámetros de configuración mínimos que se necesitan para la implementación de vCenter Server Appliance en un instancia de vCenter Server.
`embedded_vCSA_replication_on_ESXi.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de vCenter Server Appliance como un socio de replicación en otra instancia integrada de vCenter Server en un host ESXi.
`embedded_vCSA_replication_on_VC.json`	Contiene los parámetros de configuración mínimos que son obligatorios para la implementación de un socio de replicación de vCenter Server Appliance en otra instancia de vCenter Server Appliance en una instancia de vCenter Server.

Parámetros de configuración de implementación

Cuando prepare los archivos de configuración JSON para una implementación de la CLI, debe establecer parámetros y valores para proporcionar datos de entrada para la implementación de un dispositivo vCenter Server.

Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON

Los parámetros de configuración en los archivos de configuración JSON para una actualización de la CLI están organizados en secciones y subsecciones.

Tabla 2-8. Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON

Sección	Subsección	Descripción
`new_vcsa`: describe el dispositivo que desea implementar	`esxi`	Se utiliza únicamente si se desea implementar el dispositivo directamente en un host ESXi. Contiene los parámetros de configuración que describen el host ESXi de destino. Dependiendo de si desea configurar un clúster administrado de vSAN o de vLCM durante la implementación, consulte la sección correspondiente para obtener información detallada sobre los parámetros de configuración. ■ Tabla 2-9. Parámetros de configuración de la sección new_vcsa, subsección esxi para implementaciones con un clúster administrado de vSAN y de vLCM ■ Tabla 2-10. Parámetros de configuración de la Sección new_vcsa, subsección esxi para implementaciones sin un clúster administrado de vSAN o de vLCM **Nota** Es necesario completar la subsección `esxi` o `vc`.
	`vc`	Se utiliza únicamente si se desea implementar el dispositivo en el inventario de una instancia de vCenter Server. Se incluyen los parámetros de configuración que describen el host ESXi o el clúster de DRS de destino del inventario de vCenter Server. Consulte Tabla 2-11. Parámetros de configuración en la sección new_vcsa, subsección vc. **Nota** Es necesario completar la subsección `vc` o `esxi`.
	`appliance`	Se incluyen los parámetros de configuración que describen el dispositivo. Consulte Tabla 2-12. Parámetros de configuración en la sección new_vcsa, subsección appliance.
	`network`	Se incluyen los parámetros de configuración que describen la configuración de red del dispositivo. Consulte Tabla 2-13. Parámetros de configuración en la sección new_vcsa, subsección network.
	`os`	Se incluyen los parámetros de configuración que describen la configuración del sistema operativo del dispositivo. Consulte Tabla 2-14. Parámetros de configuración en la sección new_vcsa, subsección os.
	`sso`	Se incluyen los parámetros de configuración que describen la configuración de vCenter Single Sign-On para el dispositivo. Consulte Tabla 2-15. Parámetros de configuración en la sección new_vcsa, subsección sso.

Tabla 2-8. Secciones y subsecciones de los parámetros de configuración en los archivos de implementación JSON (continuación)

Sección	Subsección	Descripción
	`ovftool_arguments`	Subsección opcional para agregar argumentos arbitrarios y sus valores al comando de OVF Tool generado por el instalador. **Importante** El instalador de vCenter Server no valida los parámetros de configuración de la subsección `ovftool_arguments`. Si se establecen argumentos que OVF Tool no reconoce, es posible que se produzcan errores en la implementación.
`ceip`: describe la unión al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware.	`settings`	Se incluye solamente el parámetro de configuración `ceip_enabled` para unirse o no unirse al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware. Consulte Tabla 2-16. Parámetros de configuración en la sección ceip, subsección settings. **Nota** Si se establece en `true`, se debe ejecutar el comando de implementación de CLI con el argumento `--acknowledge-ceip`. Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administrar vCenter Server y hosts*.

Importante Los valores de cadena, incluidas las contraseñas, deben contener únicamente caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.

Para establecer un valor que contenga una barra invertida (\) o un carácter de comillas ("), debe preceder el carácter con el carácter de barra invertida (\). Por ejemplo, `"password":"my\"password"` establece la contraseña my"password. De forma similar, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYY_OVF10.ova"` establece la ruta `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0. XXXX-YYYYYYY_OVF10.ova`.

Los valores booleanos deben contener solo caracteres en minúsculas. Debe ser `true` o `false`. Por ejemplo, `"ssh_enable":false`.

Parámetros de configuración en la sección `new_vcsa`

Tabla 2-9. Parámetros de configuración de la sección `new_vcsa`, subsección `esxi` para implementaciones con un clúster administrado de vSAN y de vLCM

Nombre	Tipo	Descripción
`hostname`	string	La dirección IP o el FQDN del host ESXi de destino en el que se desea implementar el dispositivo.
`username`	string	Un nombre de usuario con privilegios administrativos en el host ESXi de destino (por ejemplo, raíz).
`password`	string	La contraseña del usuario con privilegios administrativos en el host ESXi de destino.

Tabla 2-9. Parámetros de configuración de la sección new_vcsa, subsección esxi para implementaciones con un clúster administrado de vSAN y de vLCM (continuación)

Nombre	Tipo	Descripción
deployment_network	string	El nombre de la red a la que se conectará el dispositivo. **Nota** El acceso a la red debe ser posible desde el host ESXi de destino. Se omite si el host ESXi de destino tiene una sola red.
datacenter	string	Un centro de datos específico que desea crear.
cluster	string	Nombre del clúster administrado de vSAN o de vLCM.
compression_only	Booleano	Establezca el valor en true para habilitar la compresión en el clúster de vSAN. Si este parámetro se establece en true, el parámetro deduplication_and_compression debe establecerse en false.
deduplication_and_compression	Booleano	Establezca el valor en true para habilitar la compresión y la desduplicación en el clúster de vSAN. Si este parámetro se establece en true, el parámetro compression_only debe establecerse en false.
cache_disk		Lista de los UUID o nombres canónicos de discos que desea utilizar para la memoria caché. Especifique solo los SSD.
capacity_disk		Una lista de UUID o nombres canónicos de los discos que desea utilizar para el almacenamiento. Especifique SSD o HDD.
enable_vlcm	Booleano	Establezca en true para crear un clúster administrado de vLCM.
datastore	string	El nombre del almacén de datos donde desea almacenar los archivos de configuración y los discos virtuales del dispositivo. **Nota** Debe ser posible acceder al almacén de datos desde el host ESXi. Si utiliza el modo de disco fino, el tamaño del almacén de datos debe tener un mínimo de 25 GB de espacio.
port	entero	El puerto de proxy inverso HTTPS del host ESXi de destino. El puerto predeterminado es 443. Se utiliza únicamente si el host ESXi de destino usa un puerto de proxy inverso HTTPS personalizado.

Tabla 2-10. Parámetros de configuración de la Sección new_vcsa, subsección esxi para implementaciones sin un clúster administrado de vSAN o de vLCM

Nombre	Tipo	Descripción
hostname	string	La dirección IP o el FQDN del host ESXi de destino en el que se desea implementar el dispositivo.
username	string	Un nombre de usuario con privilegios administrativos en el host ESXi de destino (por ejemplo, raíz).
password	string	La contraseña del usuario con privilegios administrativos en el host ESXi de destino.
deployment_network	string	El nombre de la red a la que se conectará el dispositivo. **Nota** El acceso a la red debe ser posible desde el host ESXi de destino. Se omite si el host ESXi de destino tiene una sola red.

Tabla 2-10. Parámetros de configuración de la Sección `new_vcsa`, subsección `esxi` para implementaciones sin un clúster administrado de vSAN o de vLCM (continuación)

Nombre	Tipo	Descripción
`datastore`	string	El nombre del almacén de datos donde desea almacenar los archivos de configuración y los discos virtuales del dispositivo. **Nota** Debe ser posible acceder al almacén de datos desde el host ESXi. Si utiliza el modo de disco fino, el tamaño del almacén de datos debe tener un mínimo de 25 GB de espacio.
`port`	entero	El puerto de proxy inverso HTTPS del host ESXi de destino. El puerto predeterminado es 443. Se utiliza únicamente si el host ESXi de destino usa un puerto de proxy inverso HTTPS personalizado.

Tabla 2-11. Parámetros de configuración en la sección `new_vcsa`, subsección `vc`

Nombre	Tipo	Descripción
`hostname`	string	La dirección IP o el FQDN de la instancia de vCenter Server de destino en el que se desea implementar el dispositivo.
`username`	string	El nombre del usuario administrador de vCenter Single Sign-On en la instancia de vCenter Server de destino, por ejemplo, administrator@vsphere.local.
`password`	string	La contraseña del usuario administrador de vCenter Single Sign-On en la instancia de vCenter Server de destino.
`deployment_network`	string	El nombre de la red a la que se conectará el dispositivo. **Nota** Debe ser posible acceder a la red desde el host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo. Se omite si el host ESXi o el clúster de DRS de destino tienen una sola red.
`datacenter`	matriz	El centro de datos de vCenter Server que contiene el host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo. Si el centro de datos se encuentra en una carpeta o una estructura de carpetas, especifique el valor como una lista de cadenas separadas por comas. Por ejemplo, `["parent_folder", "child_folder", "datacenter_name"]` **Nota** El valor distingue entre mayúsculas y minúsculas.
`datastore`	string	El nombre del almacén de datos donde desea almacenar los archivos de configuración y los discos virtuales del dispositivo. **Nota** El acceso al almacén de datos debe ser posible desde el host ESXi o el clúster de DRS de destino. El almacén de datos debe tener al menos 25 GB de espacio libre.
`port`	entero	El puerto de proxy inverso HTTPS de la instancia de vCenter Server de destino. El puerto predeterminado es 443. Se utiliza únicamente si la instancia de vCenter Server de destino usa un puerto de proxy inverso HTTPS personalizado.

Tabla 2-11. Parámetros de configuración en la sección `new_vcsa`, subsección `vc` (continuación)

Nombre	Tipo	Descripción

`target`	matriz	El host ESXi o el clúster de DRS de destino en el que se desea implementar el dispositivo.
		Importante Es necesario proporcionar el nombre que se muestra en el inventario de vCenter Server. Por ejemplo, si el nombre del host ESXi de destino es una dirección IP en el inventario de vCenter Server, no se puede proporcionar un FQDN.
		Si el host de ESXi de destino o el clúster de DRS se encuentran en una carpeta o una estructura de carpetas, especifique el valor como una lista de cadenas separadas por comas. Por ejemplo,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		Si el host de ESXi de destino forma parte de un clúster, especifique la ruta como una lista de cadenas separadas por comas. Por ejemplo,
		`["cluster_name", "esxi-host.domain.com"]`
		Nota El valor distingue entre mayúsculas y minúsculas.

`vm_folder`	string	Opcional. El nombre de la carpeta de máquina virtual en la que se implementa el dispositivo.

Tabla 2-12. Parámetros de configuración en la sección `new_vcsa`, subsección `appliance`

Nombre	Tipo	Descripción
`thin_disk_mode`	Booleano	Se establece en `true` para implementar el dispositivo con discos virtuales finos.
`deployment_option`	string	El tamaño del dispositivo. ■ Se establece en `tiny` si se desea implementar una instancia de vCenter Server Appliance para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 2 CPU, 12 GB de memoria y 315 GB de almacenamiento. ■ Se establece en `tiny-lstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 2 CPU, 12 GB de memoria y 1390 GB de almacenamiento. ■ Se establece en `tiny-xlstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 10 hosts y 100 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 2 CPU, 12 GB de memoria y 3145 GB de almacenamiento. ■ Se establece en `small` si se desea implementar una instancia de vCenter Server Appliance para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 4 CPU, 19 GB de memoria y 380 GB de almacenamiento. ■ Se establece en `small-lstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 4 CPU, 19 GB de memoria y 1435 GB de almacenamiento. ■ Se establece en `small-xlstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 100 hosts y 1.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 4 CPU, 19 GB de memoria y 3195 GB de almacenamiento. ■ Se establece en `medium` si se desea implementar una instancia de vCenter Server Appliance para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 8 CPU, 28 GB de memoria y 600 GB de almacenamiento. ■ Se establece en `medium-lstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 8 CPU, 28 GB de memoria y 1600 GB de almacenamiento.

Tabla 2-12. Parámetros de configuración en la sección `new_vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
		■ Se establece en `medium-xlstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 400 hosts y 4.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 8 CPU, 28 GB de memoria y 3360 GB de almacenamiento. ■ Se establece en `large` si se desea implementar una instancia de vCenter Server Appliance para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 16 CPU, 37 GB de memoria y 965 GB de almacenamiento. ■ Se establece en `large-lstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 16 CPU, 37 GB de memoria y 1665 GB de almacenamiento. ■ Se establece en `large-xlstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 1.000 hosts y 10.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 16 CPU, 37 GB de memoria y 3425 GB de almacenamiento. ■ Se establece en `xlarge` si se desea implementar una instancia de vCenter Server Appliance para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento predeterminado. Se implementa un dispositivo con 24 CPU, 56 GB de memoria y 1705 GB de almacenamiento. ■ Se establece en `xlarge-lstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento grande. Se implementa un dispositivo con 24 CPU, 56 GB de memoria y 1805 GB de almacenamiento. ■ Se establece en `xlarge-xlstorage` si se desea implementar una instancia de vCenter Server Appliance para hasta 2.000 hosts y 35.000 máquinas virtuales con el tamaño de almacenamiento extragrande. Se implementa un dispositivo con 24 CPU, 56 GB de memoria y 3565 GB de almacenamiento.
`image`	string	Opcional. Una dirección URL o una ruta de acceso de archivo local al paquete de instalación de vCenter Server Appliance. De forma predeterminada, el instalador utiliza el paquete de instalación que se incluye en el archivo ISO de la carpeta `vcsa`.

Tabla 2-12. Parámetros de configuración en la sección `new_vcsa`, subsección `appliance` (continuación)

Nombre	Tipo	Descripción
`name`	string	El nombre de la máquina virtual para el dispositivo. Solo se deben incluir caracteres ASCII, excepto el signo de porcentaje (%), la barra diagonal inversa (\) o la barra diagonal (/), y no se deben superar los 80 caracteres de longitud.
`ovftool_path`	string	Opcional. Una ruta de acceso de archivo local al archivo ejecutable de OVF Tool. De forma predeterminada, el instalador utiliza la instancia de OVF Tool que se incluye en el archivo ISO de la carpeta `vcsa/ovftool`.

Tabla 2-13. Parámetros de configuración en la sección `new_vcsa`, subsección `network`

Nombre	Tipo	Descripción
`ip_family`	string	La versión de IP para la red del dispositivo. Se establece en `ipv4` o `ipv6`.
`mode`	string	La asignación de IP para la red del dispositivo. Se establece en `static` o `dhcp`.
`ip`	string	La dirección IP del dispositivo. Solo se requiere si se utiliza una asignación estática, es decir, si se establece el parámetro `mode` en `static`. Es necesario establecer una dirección IPv4 o IPv6 que coincida con la versión de IP de la red, es decir, con el valor del parámetro `ip.family`. Una dirección IPv4 debe cumplir con las directrices RFC 790. Una dirección IPv6 debe cumplir con las directrices RFC 2373.

`dns_servers`	cadena o matriz	Direcciones IP de uno o varios servidores DNS.
		Para establecer más de un servidor DNS, utilice una lista de cadenas separada por comas o una lista separada por comas como una sola cadena para proporcionar la ruta de acceso. Por ejemplo,
		`["x.y.z.a", "x.y.z.b"]`
		o
		`"x.y.z.a, x.y.z.b"`
		Opcional si el parámetro `mode` se establece en `static`. No se admite cuando el modo se establece en `DHCP`.

`prefix`	string	Longitud del prefijo de red. Usar solo si el parámetro `mode` se establece en `static`. Eliminar si el parámetro `mode` se establece en `dhcp`. La longitud del prefijo de red es el número de bits que se establecen en la máscara de subred. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits en la versión binaria de la longitud del prefijo, por lo que la longitud del prefijo de red es 24. Para la versión de IPv4, el valor debe estar entre `0` y `32`. Para la versión de IPv6, el valor debe estar entre `0` y `128`.

Tabla 2-13. Parámetros de configuración en la sección `new_vcsa`, subsección `network` (continuación)

Nombre	Tipo	Descripción
`gateway`	string	Dirección IP de la puerta de enlace predeterminada. Para la versión de IPv6, el valor puede ser `default`.

`ports`	string	Opcional. Números de puerto que vCenter Server Appliance utiliza para las conexiones HTTP directas. De forma predeterminada, el puerto 80 redirecciona las solicitudes al puerto HTTPS 443. Puede personalizar los puertos HTTP y HTTPS de vCenter Server. Si desea especificar un número de puerto HTTP y HTTPS personalizado, asegúrese de no usar un puerto que ya se use en vCenter Server ni los puertos HTTP y HTTPS 80 y 443 predeterminados.
		Las opciones para especificar un puerto personalizado son: `"rhttpproxy.ext.port1":"`*`número_puerto`*`"` para el puerto HTTP y `"rhttpproxy.ext.port2:"`*`número_puerto`*`"` para el puerto HTTPS.
		El siguiente ejemplo especifica los puertos 81 y 444 para los puertos HTTP y HTTPS:
		`ports: {"rhttpproxy.ext.port1":"81",`
		`"rhttpproxy.ext.port2":"444"}`
		Para obtener más información sobre los puertos utilizados en vCenter Server, consulte Puertos necesarios en vCenter Server .

`system_name`	string	Identidad de red principal. Puede ser una dirección IP o un FQDN (de preferencia, FQDN). No se puede cambiar el valor de este parámetro después de la implementación. El FQDN y los números con punto decimal deben cumplir con las directrices RFC 1123.

Tabla 2-14. Parámetros de configuración en la sección `new_vcsa`, subsección `os`

Nombre	Tipo	Descripción
`password`	string	La contraseña del usuario raíz del sistema operativo del dispositivo. La contraseña debe tener entre 8 y 20 caracteres, y debe contener al menos uno de los siguientes tipos de carácter: una mayúscula, una minúscula, un número y un carácter especial, como por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!). Todos los caracteres deben ser caracteres ASCII inferiores sin espacios.

`ntp_servers`	cadena o matriz	Opcional. Nombres de host o direcciones IP de uno o varios servidores NTP para la sincronización de hora.
		Para establecer más de un servidor NTP, utilice una lista de cadenas separada por comas o una lista separada por comas como una sola cadena para proporcionar la ruta de acceso. Por ejemplo,
		`["x.y.z.a", "x.y.z.b"]`
		o
		`"x.y.z.a, x.y.z.b"`

Tabla 2-14. Parámetros de configuración en la sección `new_vcsa`, subsección `os` (continuación)

Nombre	Tipo	Descripción
`ssh_enable`	Booleano	Se establece en `true` para habilitar el inicio de sesión del administrador de SSH en el dispositivo. **Nota** vCenter Server Appliance de alta disponibilidad requiere acceso SSH remoto al dispositivo.
`time_tools_sync`	Booleano	Opcional. Se establece en `true` para implementar el dispositivo con la sincronización de hora de VMware Tools. VMware Tools sincroniza la hora del dispositivo con la hora del host ESXi. Se omite si los servidores NTP se establecen para la sincronización de hora; es decir, si se establece el parámetro `ntp.servers`.

Tabla 2-15. Parámetros de configuración en la sección `new_vcsa`, subsección `sso`

Nombre	Tipo	Descripción
`password`	string	Contraseña de usuario del administrador de vCenter Single Sign-On, administrator@*su_nombre_de_dominio*. Si implementa una instancia devCenter Server Appliance como la primera instancia en un dominio de vCenter Single Sign-On nuevo, debe establecer la contraseña para el usuario administrador de vCenter Single Sign-On. La contraseña debe tener entre 8 y 20 caracteres, y debe contener al menos uno de los siguientes tipos de carácter: una mayúscula, una minúscula, un número y un carácter especial, como por ejemplo, un signo de dólar ($), un numeral (#), una arroba (@), un punto (.) o un signo de exclamación (!). Todos los caracteres deben ser caracteres ASCII.
`domain_name`	string	Nombre de dominio de vCenter Single Sign-On, por ejemplo, vsphere.local. Si implementa una instancia de vCenter Server Appliance como la primera instancia en un dominio de vCenter Single Sign-On nuevo, debe establecer el nombre del dominio de vCenter Single Sign-On nuevo.
`replication_partner_hostname`	string	El nombre del sistema de la instancia de vCenter Server partner. Solo es necesario si implementa un socio de replicación en un dominio de vCenter Single Sign-On existente.
`sso_port`	entero	El puerto de proxy inverso HTTPS de la instancia de vCenter Server del socio. El puerto predeterminado es 443. Se utiliza únicamente si el socio usa un puerto de proxy inverso HTTPS personalizado.

Parámetros de configuración en la sección `ceip`

Tabla 2-16. Parámetros de configuración en la sección `ceip`, subsección `settings`

Nombre	Tipo	Descripción
`ceip_enabled`	Booleano	Se establece en `true` para unirse al CEIP para este dispositivo.

Sintaxis del comando de implementación de CLI

Puede usar argumentos de comandos para establecer los parámetros de ejecución del comando de implementación.

Puede agregar una lista de argumentos separados por un espacio en el comando de implementación de CLI.

```
vcsa-deploy install path_to_the_json_filelist_of_arguments
```

Argumento	Descripción
`--accept-eula`	Acepta el contrato de licencia de usuario final. Se requiere para ejecutar el comando de implementación.
`--acknowledge-ceip`	Confirma que el usuario acepta participar en el programa de mejora de la experiencia de cliente (CEIP) de VMware. Se requiere si el parámetro `ceip.enabled` se establece como `true` en la plantilla de implementación JSON.
`-v`, `--verbose`	Agrega información de depuración a la salida de la consola.
`-t`, `--terse`	Oculta la salida de la consola. Solo muestra mensajes de error y advertencia.
`--log-dir`*LOG_ DIR*	Establece la ubicación del registro y de otros archivos de salida.
`--skip-ovftool-verification`	Realiza una comprobación básica de los parámetros de configuración en el archivo JSON e implementa el dispositivo. No verifica los parámetros de OVF Tool.
`--no-esx-ssl-verify`	Omite la verificación de SSL para las conexiones de ESXi. **Importante** Evite utilizar esta opción, ya que puede provocar problemas durante o después de la implementación a causa de la identidad no validada del host ESXi de destino.
`--no-ssl-certificate-verification`	Omite la comprobación de certificados de seguridad de todas las conexiones de servidor.
`--operation-id`*OPERATION_ ID*	Proporciona un identificador de operación para realizar un seguimiento de las actividades de la instalación.
`--pause-on-warnings`	Realiza una pausa y espera hasta que se acepten las advertencias.
`--verify-template-only`	Realiza una comprobación de plantilla básica de los parámetros de configuración en el archivo JSON. No implementa el dispositivo.
`--precheck-only`	Solo realiza la comprobación de plantilla básica y la comprobación de parámetros de OVF Tool. No implementa el dispositivo.
`--sso-ssl-thumbprint`*SSL-SHA1-THUMBPRINT*	Valida el certificado del servidor con respecto a la huella digital SHA1 provista.

Argumento	Descripción
`-h`, `--help`	Muestra el mensaje de ayuda del comando `vcsa-deploy install`.
`--template-help`	Muestra el mensaje de ayuda para el uso de parámetros de configuración del archivo de implementación JSON.

Una vez finalizada la ejecución, se puede obtener el código de salida del comando.

Código de salida	Descripción
0	Comando ejecutado correctamente
1	Error de tiempo de ejecución
2	Error de validación
3	Error en la plantilla

Implementar vCenter Server Appliance mediante la CLI

El instalador de CLI se puede utilizar para ejecutar una implementación sin supervisión de una instancia de vCenter Server Appliance. Se debe ejecutar la implementación de CLI desde un equipo Windows, Linux o Mac que se encuentre en la misma red en la que se desea implementar el dispositivo.

Requisitos previos

- Consulte Requisitos previos para implementar vCenter Server Appliance.
- Preparar el archivo de configuración JSON para la implementación de CLI.
- Revise Sintaxis del comando de implementación de CLI.
- Compruebe que el nombre de usuario con el que inició sesión en el equipo cliente, la ruta de acceso al instalador de vCenter Server, la ruta de acceso al archivo de configuración JSON y los valores de cadena en el archivo de configuración JSON solo contengan caracteres ASCII. No se admiten los caracteres ASCII extendidos ni los caracteres que no sean ASCII.
- Para ejecutar esta utilidad en las versiones de Windows anteriores a Windows 10, es necesario instalar la versión 14.0 o posterior de las bibliotecas redistribuibles de Visual C++. Los instaladores de Microsoft de estas bibliotecas se encuentran en el directorio `vcsa\ovftool\win32\vcredist`.

Procedimiento

1 Desplácese hasta el subdirectorio `vcsa-cli-installer` del sistema operativo.

   - Si la implementación se ejecuta en un sistema operativo Windows, desplácese hasta el directorio `vcsa-cli-installer\win32`.
   - Si la implementación se ejecuta en un sistema operativo Linux, desplácese hasta el directorio `vcsa-cli-installer/lin64`.

- Si la implementación se ejecuta en el sistema operativo Mac, desplácese hasta el directorio `vcsa-cli-installer/mac`.

2 (opcional) Ejecute una comprobación previa a la implementación sin implementar el dispositivo para verificar que se haya preparado la plantilla de implementación correctamente.

```
vcsa-deploy install --precheck-only path_to_the_json_file
```

3 Ejecute el comando de implementación.

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments
path_to_the_json_file
```

Utilice *optional_arguments* para introducir argumentos separados por espacios con el fin de establecer parámetros de ejecución adicionales para el comando de implementación.

Por ejemplo, puede establecer la ubicación del registro y otros archivos de salida generados por el instalador.

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location
path_to_the_json_file
```

Implementar varias instancias de vCenter Server Appliance mediante la CLI

Puede implementar varias instancias de vCenter Server Appliance al mismo tiempo (en modo de lotes) mediante el instalador de CLI.

Para implementar varias instancias al mismo tiempo, cree plantillas JSON para todas las instancias de vCenter Server de su implementación. El instalador de CLI evalúa la topología de la implementación mediante las plantillas JSON y determina el orden. Por este motivo, las plantillas JSON deben utilizar direcciones IP estáticas para todas las instancias de vCenter Server de la implementación que dependan unas de otras.

Importante Las plantillas JSON que cree para cada dispositivo deben utilizar una dirección IP estática destinada a resolver las direcciones de red de los otros dispositivos de la implementación con los que tienen una dependencia.

Para realizar la implementación por lotes, coloque las plantillas JSON de definición de la implementación en un solo directorio. Cuando se lo invoca, el instalador de CLI pone en marcha la implementación existente con la topología definida en las plantillas JSON.

Procedimiento

1 En el área de trabajo, cree una carpeta que contenga los archivos JSON para la implementación por lotes. Por ejemplo, `*MyWorkspace*/BatchDeploy`.

2 Prepare cada archivo de configuración JSON y copie el archivo en la carpeta de la implementación por lotes. Consulte Preparar el archivo de configuración JSON para la implementación de CLI para obtener instrucciones sobre la configuración de archivos JSON.

3 Desplácese hasta el subdirectorio `vcsa-cli-installer` del sistema operativo.

- Si la implementación se ejecuta en un sistema operativo Windows, desplácese hasta el directorio `vcsa-cli-installer\win32`.
- Si la implementación se ejecuta en un sistema operativo Linux, desplácese hasta el directorio `vcsa-cli-installer/lin64`.
- Si la implementación se ejecuta en el sistema operativo Mac, desplácese hasta el directorio `vcsa-cli-installer/mac`.

4 (opcional) Ejecute una comprobación previa a la implementación sin implementar el dispositivo para verificar que se haya preparado la plantilla de implementación correctamente. Por ejemplo:

```
vcsa-deploy install --precheck-only MyWorkspace/BatchDeploy
```

5 Ejecute el comando de implementación. Por ejemplo,

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments MyWorkspace/
BatchDeploy
```

Utilice *optional_arguments* para introducir argumentos separados por espacios con el fin de establecer parámetros de ejecución adicionales para el comando de implementación.

Por ejemplo, puede establecer la ubicación del registro y otros archivos de salida generados por el instalador.

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location
MyWorkspace/BatchDeploy
```

Restaurar vCenter Server y crear una copia de seguridad de ella con base en archivos

3

vCenter Server admite un mecanismo de restauración y copia de seguridad basado en archivos que permite recuperar el entorno después de que se produzca un error.

Puede usar la interfaz de vCenter Server para crear una copia de seguridad basada en archivos de vCenter Server. Después de crear la copia de seguridad, se puede restaurar mediante el instalador de GUI del dispositivo.

La interfaz de vCenter Server se usa para realizar una copia de seguridad basada en archivos de la configuración de núcleos de vCenter Server, del inventario y de los datos históricos que elija. Los datos incluidos en la copia de seguridad se transmiten mediante FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB a un sistema remoto. La copia de seguridad no se almacena en vCenter Server.

Solo se puede realizar una restauración basada en archivos de una instancia de vCenter Server para la cual se haya hecho previamente una copia de seguridad mediante la interfaz de vCenter Server. Puede realizar esta operación de restauración mediante el instalador de GUI de vCenter Server Appliance. El proceso consiste en implementar una nueva instancia de vCenter Server Appliance y en copiar los datos de la copia de seguridad basada en archivos a un nuevo dispositivo.

Importante Si se realiza una copia de seguridad de un clúster de vCenter Server de alta disponibilidad, la operación de copia de seguridad solo copia la instancia principal de vCenter Server. Antes de restaurar un clúster de vCenter Server de alta disponibilidad, debe apagar los nodos activo, pasivo y testigo. La operación de restauración restaura la instancia de vCenter Server en el modo de vCenter Server sin alta disponibilidad. Una vez finalizada correctamente la operación de restauración, debe reconstruir el clúster.

Este capítulo incluye los siguientes temas:

Consideraciones y limitaciones para la restauración y la copia de seguridad basada en archivos

Al realizar una operación de copia de seguridad o restauración de un entorno de vCenter Server, tenga en cuenta estas consideraciones y limitaciones.

Protocolos

Las siguientes consideraciones se aplican a los protocolos de restauración y copia de seguridad basada en archivos:

- FTP y HTTP no son protocolos seguros.
- Los servidores de copia de seguridad deben admitir al menos 10 conexiones simultáneas por cada vCenter Server.
- Es necesario tener permisos de escritura para la carga y permisos de lectura para la descarga.
- Solo el modo explícito es compatible con FTPS.
- Si se usa HTTP o HTTPS, es necesario habilitar WebDAV en el servidor web de copia de seguridad.
- Solo se pueden usar FTP, FTPS, HTTP o HTTPS para transmitir datos a través de un servidor proxy HTTP.
- Es posible usar direcciones URL IPv4 e IPv6 en las operaciones de restauración y copia de seguridad basada en archivos de vCenter Server. No se admite el modo mixto de versiones de IP entre el servidor de copia de seguridad y vCenter Server.

Configuración

Después de una restauración, las siguientes configuraciones se revierten al estado que tenían cuando se realizó la copia de seguridad.

- Configuración de recursos de máquinas virtuales
- Jerarquía y configuración del grupo de recursos
- Pertenencia de clúster-host
- Reglas y configuración de DRS

Storage DRS

Si se modifica la configuración, es posible que las siguientes opciones cambien después de una restauración.

- Configuración del clúster de almacén de datos
- Pertenencia del clúster de almacén de datos
- Opciones de administración de recursos de E/S del almacén de datos (Storage I/O Control)
- Pertenencia de almacén de datos-centro de datos

- Pertenencia de host-almacén de datos

Distributed Power Management

Si se coloca un host en modo de espera después de realizar una copia de seguridad, es posible que vCenter Server obligue al host a salir del modo de espera cuando se restaure la copia de seguridad.

Conmutador virtual distribuido

Si utiliza un conmutador virtual distribuido, se recomienda exportar por separado la configuración de conmutador virtual distribuido antes de restaurar una copia de seguridad. La configuración se puede importar después de la restauración. Si no tiene en cuenta esta consideración, se podrían perder los cambios que se realicen en un conmutador virtual distribuido después de la copia de seguridad. Para conocer los pasos detallados, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2034602.

Bibliotecas de contenido

Si se eliminan bibliotecas o elementos después de realizar una copia de seguridad, no se podrá acceder a esas bibliotecas o elementos después de la restauración. Solo se podrán eliminar esas bibliotecas o elementos. Un mensaje de advertencia indicará que no se encontraron algunos archivos o carpetas en la copia de seguridad de almacenamiento.

Si se crean elementos o archivos de elementos nuevos después de realizar la copia de seguridad, no existirán registros de esos elementos en el servicio de biblioteca de contenido después de la operación de restauración. Una advertencia indicará que se encontraron archivos o carpetas adicionales en la copia de seguridad de almacenamiento.

Si se crean bibliotecas nuevas después de realizar la copia de seguridad, no existirán registros de esas bibliotecas en el servicio de biblioteca de contenido después de la restauración. El contenido de las bibliotecas existirá en la copia de seguridad de almacenamiento, pero no se mostrará ninguna advertencia. El usuario deberá limpiar manualmente las bibliotecas nuevas.

Operaciones de ciclo de vida de máquinas virtuales

- Restauración de vCenter Server a partir de una copia de seguridad realizada durante operaciones de reubicación en proceso en la instancia de vCenter Server.

  Después de restaurar vCenter Server, es posible que la vista de máquinas virtuales de vCenter Server quede desincronizada con la vista de máquinas virtuales de ESXi. Esto también sucede si la copia de seguridad se realizó durante operaciones en proceso en vCenter Server. Si las máquinas virtuales desaparecen después de restaurar vCenter Server, puede consultar los siguientes casos.

  a La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino y registrada en el host ESXi de destino, pero está huérfana o no se encuentra en el inventario de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

b La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino y no se muestra en el inventario de vCenter Server. Es necesario registrar manualmente la máquina virtual en el host ESXi y volver a agregarla al inventario de vCenter Server.

c La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino. En la instancia de vCenter Server, la máquina virtual desaparecida se marca como huérfana. Es necesario eliminar la máquina virtual del inventario de vCenter Server y agregarla de nuevo.

- Restauración de vCenter Server a partir de una copia de seguridad que tiene un diseño de máquina virtual de clon vinculado desactualizado.

  Si crea una máquina virtual de clonación vinculada después de la copia de seguridad y restaura vCenter Server desde la copia de seguridad anterior, después de la restauración, vCenter Server no conoce la existencia de la nueva máquina virtual de clonación vinculada hasta que vCenter Server detecta la nueva máquina virtual de clonación vinculada. Si se eliminan todas las máquinas virtuales existentes antes de detectar la nueva máquina virtual de clon vinculado, la eliminación de las máquinas virtuales existentes daña al nuevo clon vinculado debido a la desaparición de los discos. Para evitar esto, se debe esperar hasta que vCenter Server detecte todas las máquinas virtuales de clon vinculado antes de eliminar máquinas virtuales.

- Restaurar vCenter Server a partir de una copia de seguridad que se realizó durante el registro de la máquina virtual.

  Si registra una máquina virtual durante la copia de seguridad y restaura vCenter Server a partir de la copia de seguridad antigua, tras la restauración, la máquina virtual se marcará como huérfana en la instancia de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

vSphere High Availability

La restauración de vCenter Server a partir de una copia de seguridad puede producir una reversión a una versión anterior de estado del clúster de vSphere HA (Lista de hosts, Configuración de clúster, Estado de protección de la máquina virtual) mientras los hosts del clúster tengan la versión más reciente de estado del clúster. Debe asegurarse de que el estado del clúster de vSphere HA no sufra modificaciones durante las operaciones de restauración y copia de seguridad. De lo contrario, se pueden producir los siguientes problemas.

- Si se agregan o eliminan hosts en el clúster de vSphere HA después de una copia de seguridad y antes de la restauración de vCenter Server, es posible que las máquinas virtuales entren en conmutación por error con hosts que vCenter Server no administra, pero forman parte del clúster de HA.
- El estado de protección de las máquinas virtuales nuevas no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA. Como resultado, las máquinas virtuales quedan sin protección o desprotegidas.

- El estado de configuración de los clústeres nuevos no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA.

vCenter High Availability

La restauración de vCenter Server requiere que se vuelva a configurar vCenter HA.

Administración de almacenamiento basada en directivas

La restauración de vCenter Server a partir de una copia de seguridad puede producir las siguientes inconsistencias en directivas de almacenamiento, proveedores de almacenamiento y máquinas virtuales.

- Los proveedores de almacenamiento registrados después de la copia de seguridad se pierden.
- Los proveedores de almacenamiento no registrados después de la copia de seguridad reaparecen, y pueden mostrar otro estado del proveedor.
- Los cambios, como crear, eliminar o actualizar, realizados en las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios, como crear, eliminar o actualizar, realizados en los componentes de las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios en la configuración de directivas predeterminada para los almacenes de datos realizados después de la copia de seguridad se pierden.
- Pueden producirse cambios en la asociación de directivas de almacenamiento de la máquina virtual y sus discos, y en su cumplimiento de las directivas.

Red de área de almacenamiento virtual

La restauración de vCenter Server a partir de una copia de seguridad puede provocar inconsistencias en vSAN. Para obtener información sobre la forma de comprobar el estado de vSAN, consulte *Administrar VMware vSAN*.

Aplicación de revisiones

La restauración de vCenter Server a partir de una copia de seguridad puede producir la desaparición de revisiones de seguridad. Debe volver a aplicarlas una vez se complete la restauración. Para obtener información sobre la aplicación de revisiones en vCenter Server, consulte *Actualizar vSphere*.

Programar una copia de seguridad basada en archivos

Puede programar copias de seguridad basadas en archivos para vSphere 6.7 y versiones posteriores. Puede configurar una programación que se utilice para realizar copias de seguridad periódicas.

La programación puede configurarse con los datos sobre la ubicación de copia de seguridad, el patrón de repetición y la retención de las copias de seguridad.

Solo puede configurar una programación a la vez.

Requisitos previos

- Debe tener un servidor FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB en funcionamiento con suficiente espacio de disco para poder almacenar la copia de seguridad.

Procedimiento

1 En un explorador web, vaya a la interfaz de administración de vCenter Server, https://*dirección-IP-o-dominio-completo-de-dispositivo*:5480.

2 Inicie sesión como raíz.

3 En la interfaz de administración de vCenter Server, haga clic en **Copia de seguridad**.

4 Haga clic en **Configurar** para definir una programación de copia de seguridad.

5 Introduzca los detalles de ubicación de la copia de seguridad.

Opción	Descripción
Ubicación de la copia de seguridad	Introduzca la ubicación de la copia de seguridad, incluido el protocolo que se debe usar para conectarse al servidor de copia de seguridad, el puerto, la dirección del servidor y la carpeta de copias de seguridad donde se almacenarán los archivos de copia de seguridad. Utilice uno de los siguientes protocolos: FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB. Para FTP, FTPS, HTTP o HTTPS, la ruta de acceso depende del directorio de inicio configurado para el servicio.
Credenciales del servidor de copia de seguridad	Escriba el nombre de usuario y la contraseña de un usuario con privilegios de **escritura** en el servidor de copia de seguridad.

6 Establezca la repetición de la programación y la hora para la copia de seguridad.

La repetición se puede establecer de forma diaria o semanal, o puede personalizar la programación para ejecutar la copia de seguridad en un determinado día o días de la semana. Puede especificar la hora del día para ejecutar la copia de seguridad. La hora predeterminada es 23:59.

7 (opcional) Introduzca una contraseña de cifrado si desea cifrar el archivo de copia de seguridad.

Si elige cifrar los datos de copia de seguridad, deberá usar la contraseña de cifrado para el proceso de restauración.

8 Seleccione **Conservar todas las copias de seguridad** o introduzca el número de copias de seguridad que se retendrán.

La información de retención proporciona el número de copias de seguridad que se retendrán para una instancia determinada de vCenter Server.

9 (opcional) Seleccione **Estadísticas, eventos y tareas** para hacer una copia de seguridad adicional de los datos históricos de la base de datos.

10 Haga clic en **Crear**.

La información de programación de copia de seguridad se rellena en la página Copia de seguridad.

Resultados

Las copias de seguridad completas y en curso se enumeran debajo de Actividad.

Pasos siguientes

Puede realizar una copia de seguridad inmediata con la información de programación existente si selecciona **Utilizar la ubicación de copia de seguridad y el nombre de usuario de la programación de copia de seguridad** en el cuadro de diálogo Realizar copia de seguridad ahora.

Realizar manualmente una copia de seguridad de vCenter Server mediante la interfaz de administración de vCenter Server

Se puede usar la interfaz de administración de vCenter Server para realizar una copia de seguridad de la instancia de vCenter Server. Puede seleccionar si el archivo de copia de seguridad incluirá datos históricos, como estadísticas, eventos y tareas.

Nota La operación de copia de seguridad de un clúster de vCenter High Availability solo incluye al nodo activo.

Requisitos previos

- Debe tener un servidor FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB en funcionamiento con suficiente espacio de disco para poder almacenar la copia de seguridad.

Procedimiento

1 En un explorador web, vaya a la interfaz de administración de vCenter Server, https://*dirección-IP-o-dominio-completo-de-dispositivo*:5480.

2 Inicie sesión como raíz.

3 En la interfaz de administración de vCenter Server, haga clic en **Copia de seguridad**.

La tabla ubicada debajo de Actividad muestra la versión más reciente de la copia de seguridad creada a partir de vCenter Server.

4 Haga clic en **Realizar copia de seguridad ahora**.

Se abrirá el asistente **Copia de seguridad de dispositivo**.

5 (opcional) Seleccione **Utilizar nombre de usuario y ubicación de copia de seguridad de la programación de copia de seguridad** para usar la información de una copia de seguridad programada.

6 Introduzca los detalles de ubicación de la copia de seguridad.

Opción	Descripción
Ubicación de la copia de seguridad	Introduzca la ubicación de la copia de seguridad, incluido el protocolo que se debe usar para conectarse al servidor de copia de seguridad, el puerto, la dirección del servidor y la carpeta de copias de seguridad donde se almacenarán los archivos de copia de seguridad. Utilice uno de los siguientes protocolos: FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB. Para FTP, FTPS, HTTP o HTTPS, la ruta de acceso depende del directorio de inicio configurado para el servicio.
Credenciales del servidor de copia de seguridad	Escriba el nombre de usuario y la contraseña de un usuario con privilegios de **escritura** en el servidor de copia de seguridad. **Nota** El nombre de usuario y la contraseña deben contener solo caracteres ASCII.

7 (opcional) Introduzca una contraseña de cifrado si desea cifrar el archivo de copia de seguridad.

Si elige cifrar los datos de copia de seguridad, deberá usar la contraseña de cifrado para el proceso de restauración.

8 (opcional) Seleccione **Estadísticas, eventos y tareas** para hacer una copia de seguridad adicional de los datos históricos de la base de datos.

9 (opcional) En el cuadro de diálogo **Descripción**, escriba una descripción para la copia de seguridad.

10 Haga clic en **Iniciar** para comenzar el proceso de copia de seguridad.

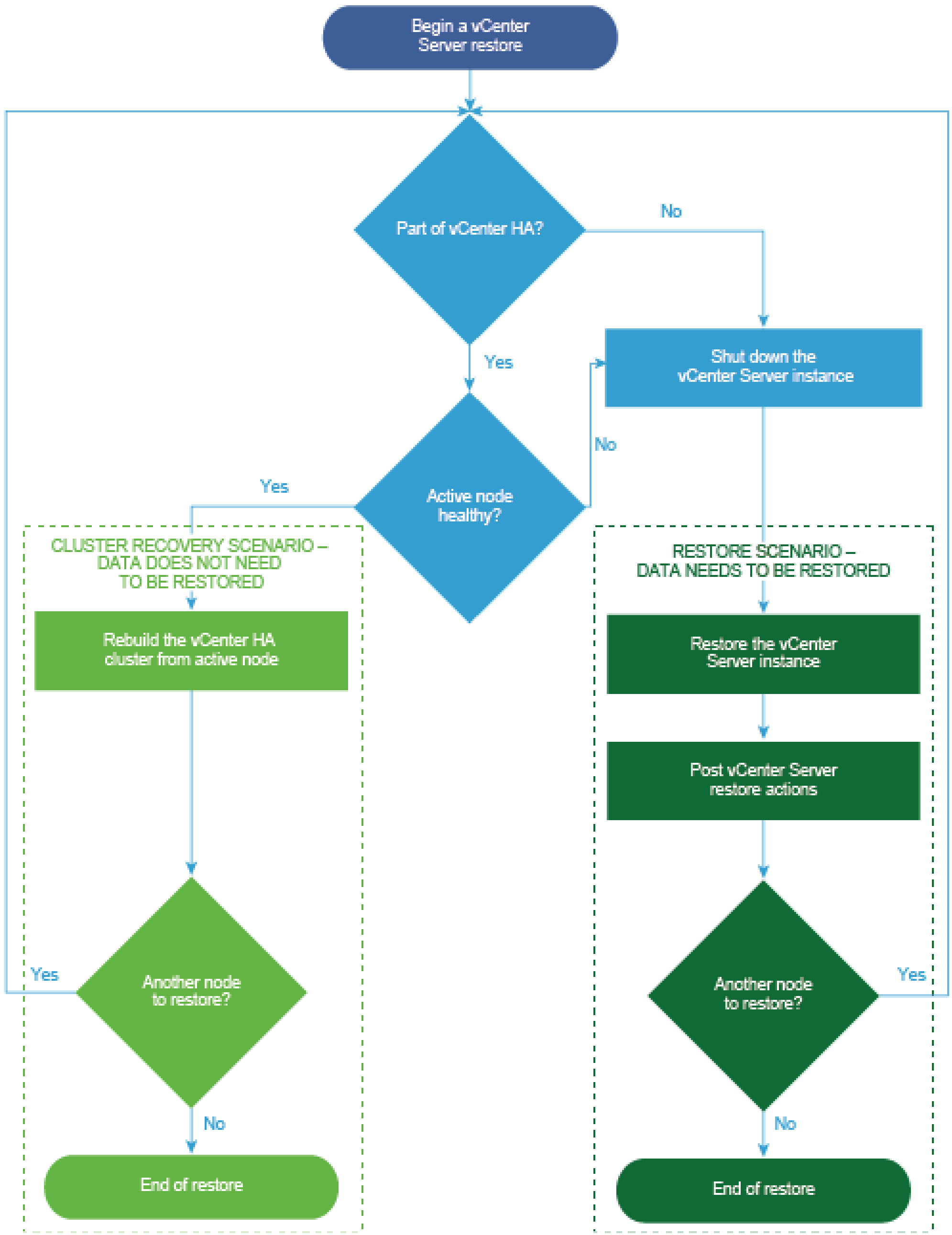
Resultados

Las copias de seguridad completas y en curso se enumeran debajo de Actividad.

Restaurar vCenter Server desde una copia de seguridad basada en archivos

Puede usar el instalador de GUI de vCenter Server Appliance para restaurar una instancia de vCenter Server en un host ESXi o en una instancia de vCenter Server. El procedimiento de restauración tiene dos etapas. En la primera etapa, se implementa una nueva instancia de vCenter Server Appliance. En la segunda etapa, se rellena la instancia de vCenter Server Appliance que se acaba de implementar con los datos almacenados en la copia de seguridad basada en archivos.

Figura 3-1. Flujo de trabajo de restauración de vCenter Server



Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software. Consulte .

- Si la instancia de vCenter Server forma parte de un clúster de vCenter High Availability, debe apagar los nodos activo, pasivo y testigo del clúster antes de restaurar vCenter Server.

Procedimiento

1 Etapa 1: Implementar un nuevo dispositivo

   En la etapa 1 del proceso de restauración, se implementa el archivo OVA, que está incluido en el instalador de GUI de vCenter Server.

2 Etapa 2: Transferir datos al dispositivo recién implementado

   Cuando termina la implementación de OVA, se lo redirige a la etapa 2 del proceso de restauración, en el cual los datos de la ubicación de la copia de seguridad se copian en la instancia de vCenter Server Appliance recién implementada.

Etapa 1: Implementar un nuevo dispositivo

En la etapa 1 del proceso de restauración, se implementa el archivo OVA, que está incluido en el instalador de GUI de vCenter Server.

Como alternativa a realizar la primera etapa de la restauración con el instalador de GUI, puede implementar el archivo OVA de la nueva instancia de vCenter Server Appliance o usar vSphere Client. Después de la implementación de OVA, debe iniciar sesión en la interfaz de administración de vCenter Server del dispositivo recién implementado para seguir con la segunda etapa del proceso de restauración. Consulte "Implementar una plantilla de OVF o de OVA" en *Administrar máquinas virtuales de vSphere* Administrar máquinas virtuales de vSphere para obtener información sobre la implementación de un archivo OVA mediante vSphere Client.

Requisitos previos

- Descargue el instalador de vCenter Server y móntelo. Consulte Descargar el instalador de vCenter Server y montarlo.

  Nota Si va a restaurar una copia de seguridad de un producto que tiene aplicada una revisión de producto de vCenter Server, debe descargar el archivo ISO completo de esa revisión en particular. Consulte Descargar VMware vSphere.

- Si planea restaurar vCenter Server en un host ESXi, compruebe que el host ESXi de destino no esté en el modo de bloqueo o de mantenimiento y que no forme parte de un clúster de DRS completamente automatizado.
- Si desea restaurar vCenter Server en un clúster de DRS de un inventario de vCenter Server, compruebe que el clúster contenga al menos un host ESXi que no esté en modo de bloqueo o de mantenimiento.
- Si desea asignar una dirección IP estática al dispositivo, compruebe que se hayan configurado los registros de DNS inversos y directos para la dirección IP.
- Si intenta restaurar una instancia de vCenter Server que aún está en ejecución, antes de iniciar la operación de restauración debe apagar la instancia de vCenter Server incluida en la copia de seguridad.

Procedimiento

1 En el instalador de vCenter Server, desplácese hasta el directorio `vcsa-ui-installer`, vaya al subdirectorio del sistema operativo y ejecute el instalador.

- En un sistema operativo Windows, vaya al subdirectorio `win32` y ejecute el archivo `installer.exe`.
- En un sistema operativo Linux, vaya al subdirectorio `lin64` y ejecute el archivo `installer`.
- En un sistema operativo Mac OS, vaya al subdirectorio `mac` y ejecute el archivo `Installer.app`.

2 En la página de inicio, haga clic en **Restaurar**.

3 Revise la página de introducción para comprender el proceso de restauración y haga clic en **Siguiente**.

4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.

5 En la página Introducir los detalles de la copia de seguridad, introduzca los detalles del archivo de copia de seguridad que desea restaurar y haga clic en **Siguiente**.

Opción	Descripción
Ubicación de la copia de seguridad	Introduzca la dirección del servidor y la carpeta de copia de seguridad donde están almacenados los archivos de copia de seguridad. También puede introducir la dirección IP o el nombre de host del servidor de copia de seguridad y buscar la ubicación de la carpeta de copias de seguridad. Seleccione el protocolo que desea usar para recuperar la copia de seguridad del servidor de copia de seguridad. Puede seleccionar FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB. Por ejemplo: `ftp://<server_IP_address>/tmp/vCenter/hostname_vcenter.com/<backup_filename>`
Nombre de usuario	Escriba el nombre de usuario de un usuario con privilegios de **lectura** sobre el servidor de copia de seguridad.
Contraseña	Escriba la contraseña del usuario con privilegios de **lectura** sobre el servidor de copia de seguridad.

6 Revise la información de la copia de seguridad y haga clic en **Siguiente**.

7 Conéctese al host ESXi o a la instancia de vCenter Server en la cual desea implementar la instancia de vCenter Server Appliance que usará para la operación de restauración.

Opción	Pasos
Puede conectarse al host ESXi en el que desea implementar el dispositivo que usará para la operación de restauración.	1 Escriba el FQDN o la dirección IP del host ESXi. 2 Especifique el puerto HTTPS del host ESXi. 3 Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en el host ESXi de destino y haga clic en **Sí** para aceptar la huella digital del certificado.
Puede conectarse a una instancia de vCenter Server y examinar el inventario para seleccionar el host ESXi o el clúster de DRS donde desea implementar el dispositivo que usará para la operación de restauración.	1 Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server. 2 Especifique el puerto HTTPS de la instancia de vCenter Server. 3 Especifique el nombre de usuario y la contraseña de un usuario con privilegios administrativos de vCenter Single Sign-On en la instancia de vCenter Server (por ejemplo, el usuario administrator@*su_nombre_de_dominio*). 4 Haga clic en **Siguiente**. 5 Asegúrese de que la advertencia de certificado muestre la huella digital SHA1 del certificado SSL que se instaló en la instancia de vCenter Server de destino y haga clic en **Sí** para aceptar la huella digital del certificado. 6 Seleccione el centro de datos o la carpeta de centro de datos que contienen el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**. **Nota** Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento. 7 Seleccione el host ESXi o el clúster de DRS donde desea implementar el dispositivo y haga clic en **Siguiente**.

8 Acepte la advertencia de certificado.

9 Escriba un nombre para vCenter Server Appliance, establezca la contraseña del usuario raíz y haga clic en **Siguiente**.

10 Seleccione el tamaño de implementación de la nueva instancia de vCenter Server Appliance según el tamaño del inventario de vSphere.

Opción de tamaño de implementación	Descripción
Muy pequeño	Implementa un dispositivo con 2 vCPU y 12 GB de memoria. Apropiado para entornos con hasta 10 hosts o 100 máquinas virtuales.
Pequeño	Implementa un dispositivo con 4 CPU y 19 GB de memoria. Apropiado para entornos con hasta 100 hosts o 1.000 máquinas virtuales.
Mediano	Implementa un dispositivo con 8 CPU y 28 GB de memoria. Apropiado para entornos con hasta 400 hosts o 4.000 máquinas virtuales.

Opción de tamaño de implementación	Descripción
Grande	Implementa un dispositivo con 16 CPU y 37 GB de memoria. Apropiado para entornos con hasta 1.000 hosts o 10.000 máquinas virtuales.
Extragrande	Implementa un dispositivo con 24 CPU y 56 GB de memoria. Apropiado para entornos con hasta 2.500 hosts o 45.000 máquinas virtuales.

11 Seleccione el tamaño de almacenamiento de la nueva instancia de vCenter Server Appliance y haga clic en **Siguiente**.

Importante Debe tener en cuenta el tamaño de almacenamiento del dispositivo que desea restaurar.

Opción de tamaño de almacenamiento	Descripción de tamaño de implementación muy pequeño	Descripción de tamaño de implementación pequeño	Descripción de tamaño de implementación mediano	Descripción de tamaño de implementación grande	Descripción de tamaño de implementación extragrande
Predeterminado	Implementa un dispositivo con 315 GB de almacenamiento.	Implementa un dispositivo con 380 GB de almacenamiento.	Implementa un dispositivo con 600 GB de almacenamiento.	Implementa un dispositivo con 965 GB de almacenamiento.	Implementa un dispositivo con 1705 GB de almacenamiento.
Grande	Implementa un dispositivo con 1390 GB de almacenamiento.	Implementa un dispositivo con 1435 GB de almacenamiento.	Implementa un dispositivo con 1600 GB de almacenamiento.	Implementa un dispositivo con 1665 GB de almacenamiento.	Implementa un dispositivo con 1.805 GB de almacenamiento.
Extragrande	Implementa un dispositivo con 3145 GB de almacenamiento.	Implementa un dispositivo con 3195GB de almacenamiento.	Implementa un dispositivo con 3360 GB de almacenamiento.	Implementa un dispositivo con 3425 GB de almacenamiento.	Implementa un dispositivo con 3565 GB de almacenamiento.

12 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

13 En la página Ajustar la configuración de red, revise la configuración que se carga a partir del archivo de copia de seguridad de vCenter Server.

14 (opcional) Edite la configuración de red para que coincida con el entorno de red actual donde está almacenado el dispositivo de vCenter Server.

15 En la página Listo para finalizar la etapa 1, revise la configuración de implementación de la instancia de vCenter Server Appliance restaurada y haga clic en **Finalizar** para iniciar el proceso de implementación de OVA.

16 Espere a que finalice la implementación de OVA y haga clic en **Continuar** para pasar a la etapa 2 del proceso de restauración a fin de transferir los datos al dispositivo recién implementado.

Nota Si hace clic en **Cerrar** para salir del asistente, deberá iniciar sesión en la interfaz de administración de vCenter Server para transferir los datos.

Resultados

La instancia de vCenter Server Appliance recién implementada se ejecuta en el servidor de destino, pero los datos no se copian desde la ubicación de la copia de seguridad.

Etapa 2: Transferir datos al dispositivo recién implementado

Cuando termina la implementación de OVA, se lo redirige a la etapa 2 del proceso de restauración, en el cual los datos de la ubicación de la copia de seguridad se copian en la instancia de vCenter Server Appliance recién implementada.

Procedimiento

1 Revise la introducción a la etapa 2 del proceso de restauración y haga clic en **Siguiente**.

2 Revise los detalles de la copia de seguridad y haga clic en **Siguiente**.

3 Si va a restaurar un nodo que admite Enhanced Linked Mode para vCenter Server Appliance, se le solicitará que proporcione las credenciales de Single Sign-On. Introduzca el nombre de usuario y la contraseña de Single Sign-On y, a continuación, haga clic en **Validar y recuperar**.

4 En la página Listo para finalizar, revise los detalles, haga clic en **Finalizar** y, luego, en **Aceptar** para completar la etapa 2 del proceso de restauración.

   Este proceso reinicia el servicio de administración de vCenter Server. No se puede acceder a la API de administración de vCenter Server durante el reinicio.

   Importante Si se produce un error en la operación de restauración de una máquina virtual de vCenter Server Appliance, debe apagar la máquina virtual restaurada parcialmente y eliminarla. A continuación, podrá intentar restaurar la máquina virtual de nuevo.

5 (opcional) Después de que se complete el proceso de restauración, haga clic en **https://*vcenter_server_appliance_fqdn*/ui** para ir a vSphere Client e iniciar sesión en la instancia de vCenter Server o bien haga clic en **https://*vcenter_server_appliance_fqdn*:443** para ir a la página Introducción de vCenter Server.

6 Haga clic en **Cerrar** para cerrar el asistente.

   Se abrirá la página de introducción de vCenter Server.

7 Si el nodo de vCenter con copia de seguridad forma parte de un clúster de vCenter High Availability, es necesario volver a configurar el clúster una vez que la operación de restauración se complete correctamente.

   Para obtener información sobre cómo realizar operaciones de copia de seguridad y restauración, consulte *Disponibilidad de vSphere*.

Pasos siguientes

Después de completar correctamente la operación de restauración, en caso de que se produzca una pérdida total del almacenamiento y de todos los servidores donde se pierdan todos los datos o el hardware físico, siga las instrucciones del artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/76585 para recuperar el estado previo a la restauración del sistema en el momento de la copia de seguridad.

Restaurar y crear copias de seguridad con base en imágenes de un entorno de vCenter Server

4

Con las API de vSphere y un producto de terceros, se puede hacer una copia de seguridad y una restauración de la máquina virtual que contiene vCenter Server.

Puede realizar una copia de seguridad de imagen completa de una máquina virtual que contiene vCenter Server. La máquina virtual debe usar un FQDN con la resolución de DNS correcta, o el nombre de host debe estar configurado para ser una dirección IP.

Este capítulo incluye los siguientes temas:

Consideraciones y limitaciones para copias de seguridad y restauraciones basadas en imágenes

Al restaurar un entorno de vCenter Server, tenga en cuenta estas consideraciones y limitaciones.

Nota La restauración de una instancia de vCenter Server con configuración de red DHCP provoca una modificación en su dirección IP. La dirección IP modificada impide que algunos servicios de vCenter Server se inicien correctamente. Para iniciar correctamente todos los servicios de vCenter Server, después de la restauración, se debe volver a configurar la dirección IP de la instancia de vCenter Server restaurada con la dirección IP que tenía esta instancia cuando se realizó la copia de seguridad.

Sincronizar los relojes con la sincronización de hora de NTP antes de la copia de seguridad

Antes de crear una copia de seguridad de la implementación de vCenter Server, compruebe que todos los componentes de la red de vSphere tengan los relojes sincronizados mediante la sincronización de hora de NTP. Consulte Sincronizar los relojes en la red de vSphere.

Configuración

Después de una restauración, las siguientes configuraciones se revierten al estado que tenían cuando se realizó la copia de seguridad.

- Configuración de recursos de máquinas virtuales
- Jerarquía y configuración del grupo de recursos
- Pertenencia de clúster-host
- Reglas y configuración de DRS

Storage DRS

Si se modifica la configuración, es posible que las siguientes opciones cambien después de una restauración.

- Configuración del clúster de almacén de datos
- Pertenencia del clúster de almacén de datos
- Opciones de administración de recursos de E/S del almacén de datos (Storage I/O Control)
- Pertenencia de almacén de datos-centro de datos
- Pertenencia de host-almacén de datos

Distributed Power Management

Si se coloca un host en modo de espera después de realizar una copia de seguridad, es posible que vCenter Server obligue al host a salir del modo de espera cuando se restaure la copia de seguridad.

Conmutador virtual distribuido

Si utiliza un conmutador virtual distribuido, se recomienda exportar por separado la configuración de conmutador virtual distribuido antes de restaurar una copia de seguridad. La configuración se puede importar después de la restauración. Si no tiene en cuenta esta consideración, se podrían perder los cambios que se realicen en un conmutador virtual distribuido después de la copia de seguridad. Para conocer los pasos detallados, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2034602.

Bibliotecas de contenido

Si se eliminan bibliotecas o elementos después de realizar una copia de seguridad, no se podrá acceder a esas bibliotecas o elementos después de la restauración. Solo se podrán eliminar esas bibliotecas o elementos. Un mensaje de advertencia indicará que no se encontraron algunos archivos o carpetas en la copia de seguridad de almacenamiento.

Si se crean elementos o archivos de elementos nuevos después de realizar la copia de seguridad, no existirán registros de esos elementos en el servicio de biblioteca de contenido después de la operación de restauración. Una advertencia indicará que se encontraron archivos o carpetas adicionales en la copia de seguridad de almacenamiento.

Si se crean bibliotecas nuevas después de realizar la copia de seguridad, no existirán registros de esas bibliotecas en el servicio de biblioteca de contenido después de la restauración. El contenido de las bibliotecas existirá en la copia de seguridad de almacenamiento, pero no se mostrará ninguna advertencia. El usuario deberá limpiar manualmente las bibliotecas nuevas.

Operaciones de ciclo de vida de máquinas virtuales

- Restauración de vCenter Server desde una copia de seguridad que se realizó mientras había operaciones de reubicación en proceso dentro de la instancia de vCenter Server.

  Después de restaurar vCenter Server, la vista de vCenter Server de las máquinas virtuales puede estar desincronizada con la vista de ESXi de las máquinas virtuales. Esto también sucede si realizó la copia de seguridad mientras había operaciones en proceso en la instancia de vCenter Server. Si las máquinas virtuales desaparecen después de restaurar vCenter Server, puede consultar los siguientes casos.

  a La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino y registrada en el host ESXi de destino, pero no se muestra en el inventario de vCenter Server. Es necesario agregar manualmente la máquina virtual al inventario de vCenter Server.

  b La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino y no se muestra en el inventario de vCenter Server. Debe registrar manualmente la máquina virtual en la instancia de ESXi y agregarla nuevamente al inventario de vCenter Server.

  c La máquina virtual desaparecida se encuentra ubicada en el host ESXi de destino, pero no está registrada en el host ESXi de destino. Dentro de la instancia de vCenter Server, la máquina virtual que falta está marcada como huérfana. Es necesario eliminar la máquina virtual del inventario de vCenter Server y agregarla de nuevo.

- Restauración de vCenter Server desde una copia de seguridad que posee un diseño desactualizado de máquina virtual de clonación vinculada.

  Si crea una máquina virtual de clonación vinculada después de la copia de seguridad y restaura vCenter Server desde la copia de seguridad anterior, después de la restauración, vCenter Server no conoce la existencia de la nueva máquina virtual de clonación vinculada hasta que vCenter Server detecta la nueva máquina virtual de clonación vinculada. Si se eliminan todas las máquinas virtuales existentes antes de detectar la nueva máquina virtual de clon vinculado, la eliminación de las máquinas virtuales existentes daña al nuevo clon vinculado debido a la desaparición de los discos. Para evitar esta situación, debe esperar hasta que vCenter Server detecte todas las máquinas virtuales de clonación vinculada antes de eliminar las máquinas virtuales.

vSphere High Availability

La restauración de vCenter Server desde una copia de seguridad puede provocar una reversión a una versión anterior en el estado del clúster de vSphere HA (HostList, ClusterConfiguration, estado de protección de la máquina virtual) mientras los hosts en el clúster tienen la versión más reciente del estado del clúster. Asegúrese de que el estado del clúster de vSphere HA no sufra modificaciones durante las operaciones de restauración y copia de seguridad. De lo contrario, se pueden hacer presentes los siguientes problemas.

- Si se agregan o se eliminan hosts en el clúster de vSphere HA después de un copia de seguridad y antes de la restauración de vCenter Server, las máquinas virtuales potencialmente podrían conmutar por error a hosts que no son administrados por vCenter Server, pero siguen formando parte del clúster de HA.
- Los estados de protección para las nuevas máquinas virtuales no se actualizan en los agentes de vSphere HA presentes en los hosts que forman parte del clúster de vSphere HA. Como resultado, las máquinas virtuales quedan sin protección o desprotegidas.
- El estado de configuración de los clústeres nuevos no se actualiza en agentes de vSphere HA en hosts que forman parte de un clúster de vSphere HA.

vCenter High Availability

La restauración de vCenter Server requiere que se vuelva a configurar vCenter HA.

Administración de almacenamiento basada en directivas

La restauración de vCenter Server a partir de una copia de seguridad puede producir las siguientes inconsistencias en directivas de almacenamiento, proveedores de almacenamiento y máquinas virtuales.

- Los proveedores de almacenamiento registrados después de la copia de seguridad se pierden.
- Los proveedores de almacenamiento no registrados después de la copia de seguridad reaparecen y podrían mostrar otro estado del proveedor.
- Los cambios, como crear, eliminar o actualizar, realizados en las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios, como crear, eliminar o actualizar, realizados en los componentes de las directivas de almacenamiento después de la copia de seguridad se pierden.
- Los cambios en la configuración de directivas predeterminada para los almacenes de datos realizados después de la copia de seguridad se pierden.
- Pueden producirse cambios en la asociación de directivas de almacenamiento de la máquina virtual y sus discos, y en su cumplimiento de las directivas.

Red de área de almacenamiento virtual

La restauración de vCenter Server desde una copia de seguridad puede provocar incoherencias en vSAN. Para obtener información sobre cómo comprobar el estado de vSAN, consulte *Administrar VMware vSAN*.

Aplicación de revisiones

La restauración de vCenter Server a partir de una copia de seguridad puede producir la desaparición de revisiones de seguridad. Debe volver a aplicarlas una vez se complete la restauración. Para obtener información sobre la aplicación de revisiones a vCenter Server Appliance, consulte *Actualizar vSphere*.

Restaurar un entorno de vCenter Server basado en imágenes

Puede utilizar un producto de terceros que haga uso de las API de vSphere para restaurar una máquina virtual que contenga vCenter Server.

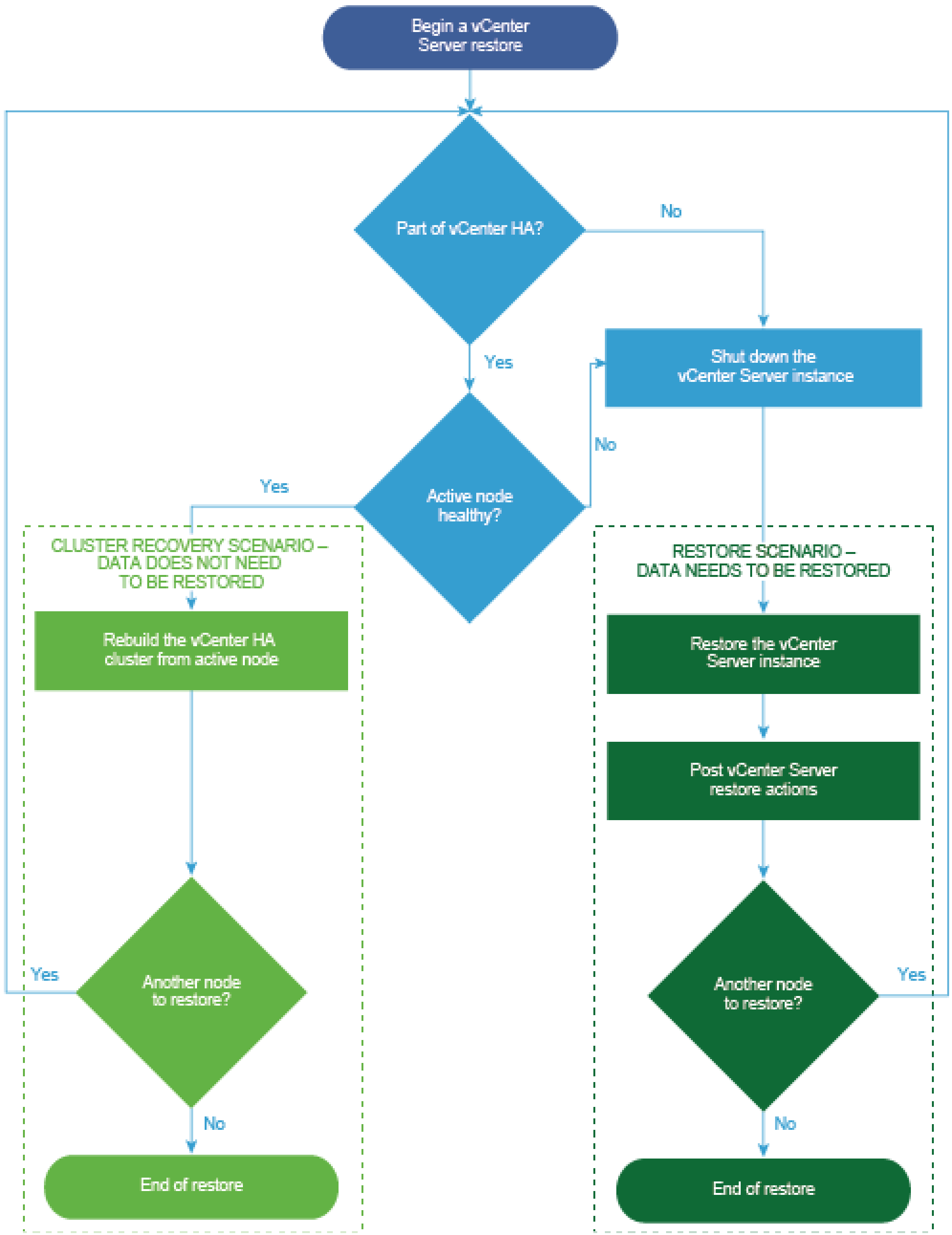
Puede realizar una restauración basada en imágenes de una máquina virtual que contenga vCenter Server. La máquina virtual debe usar un FQDN con la resolución de DNS correcta, o el nombre de host del equipo debe estar configurado para ser una dirección IP.

Para restaurar una máquina virtual en la ubicación original, sobrescriba la máquina virtual con copia de seguridad o cree una nueva que contenga la instancia restaurada de vCenter Server en el mismo host ESXi. También puede restaurar la máquina virtual en un nuevo host ESXi.

Puede restaurar una máquina virtual que contenga una instancia de vCenter Server directamente en el host ESXi que ejecuta el dispositivo de otro proveedor cuando el servicio de vCenter Server deja de estar disponible o cuando no se puede acceder a la interfaz de usuario de otro proveedor mediante vSphere Client.

Importante No se admite la restauración de máquinas virtuales que tienen instantáneas o que están configuradas con Fault Tolerance.

Figura 4-1. Flujo de trabajo de restauración de vCenter Server



Restaurar una instancia de vCenter Server

Puede utilizar un producto de terceros para restaurar un entorno de vCenter Server.

Importante Solo puede hacer copias de seguridad de máquinas virtuales que contengan instancias de vCenter Server y restaurarlas. No se puede hacer copias de seguridad ni restaurar máquinas físicas que ejecuten vCenter Server mediante un producto de terceros.

Procedimiento

1. Restaure la máquina virtual de vCenter Server en el host ESXi con una solución de terceros.
2. Use el comando `service-control --status --all` para verificar que se hayan iniciado los servicios.

   Espere a que se inicien todos los servicios de vCenter Server, lo que puede tardar varios minutos.
3. Inicie sesión en la interfaz de administración de vCenter Server, https://*dirección-IP-o-dominio-completo-de-dispositivo*:5480.
4. Ejecute la operación de conciliación y proporcione las credenciales de Single Sign-On.

Pasos siguientes

Encienda la máquina virtual restaurada donde se encuentra la instancia de vCenter Server restaurada.

Restaurar un entorno de vCenter Enhanced Linked Mode

Puede restaurar un entorno de vCenter Enhanced Linked Mode mediante una solución de terceros.

Importante Solo puede hacer copias de seguridad de máquinas virtuales que contengan instancias de vCenter Server y restaurarlas. No se puede hacer copias de seguridad ni restaurar máquinas físicas que ejecuten vCenter Server mediante un producto de terceros.

Procedimiento

1. Restaure la máquina virtual de vCenter Server en el host ESXi con una solución de terceros.

   Los servicios están enmascarados y aún no están en ejecución.
2. Use el comando `systemctl status applmgmt` para comprobar que se ha iniciado la instancia `systemd` del servicio `applmgmt`.

   Espere a que se inicien todos los servicios de vCenter Server, lo que puede tardar varios minutos.
3. Inicie sesión en la interfaz de administración de vCenter Server, https://*dirección-IP-o-dominio-completo-de-dispositivo*:5480.

Pasos siguientes

Encienda la máquina virtual restaurada donde se encuentra la instancia de vCenter Server restaurada.

Después de implementar vCenter Server Appliance

5

Después de implementar vCenter Server Appliance, tenga en cuenta estas opciones posteriores a la instalación antes de agregar el inventario que administrará vCenter Server.

Para obtener información sobre cómo configurar el servicio vSphere Authentication Proxy, consulte *vSphere Security*.

Para obtener información sobre la actualización de vCenter Server, consulte *Actualización de vCenter Server*.

Este capítulo incluye los siguientes temas:

Iniciar sesión en vCenter Server con vSphere Client

Inicie sesión en vCenter Server con vSphere Client para administrar su inventario de vSphere.

En vSphere 6.5 y versiones posteriores, vSphere Client se instala como parte de la implementación de vCenter Server Appliance. De esta manera, vSphere Client siempre apunta a la misma instancia de vCenter Single Sign-On.

Procedimiento

1 Abra un explorador web e introduzca la URL de la instancia de vCenter Server: **https://*dirección_IP_o_FQDN_de_vCenter_Server***

2 Seleccione **Iniciar vSphere Client (HTML5)**.

   En lugar de eso, puede abrir un explorador web e introducir la URL de vSphere Client: **https://*dirección_IP_o_FQDN_de_vCenter_Server*/ui**.

3 Introduzca las credenciales de un usuario que tenga permisos en vCenter Server y haga clic en **Iniciar sesión**.

4 Si aparece un mensaje de advertencia acerca de un certificado SSL que no es de confianza, seleccione la acción correcta según su directiva de seguridad.

Opción	Acción
Omita la advertencia de seguridad para esta sesión de inicio de sesión solamente.	Haga clic en **Omitir**.
Omita la advertencia de seguridad para esta sesión de inicio de sesión e instale el certificado predeterminado para que la advertencia no vuelva a aparecer.	Seleccione **Instalar este certificado y no mostrar ninguna advertencia de seguridad para este servidor** y haga clic en **Omitir**. Seleccione esta opción solamente si al usar el certificado predeterminado no se presenta un problema de seguridad en el entorno.
Cancele e instale un certificado firmado antes de continuar.	Haga clic en **Cancelar** y asegúrese de que esté instalado un certificado firmado en el sistema de vCenter Server antes de intentar volver a conectarse.

5 Para cerrar sesión, haga clic en el nombre de usuario en la parte superior de la ventana de vSphere Client y seleccione **Cerrar sesión**.

Resultados

vSphere Client conecta todos los sistemas devCenter Server para los que el usuario especificado tiene permisos, y así permite ver y administrar el inventario.

Instalar el complemento de autenticación mejorado de VMware

El complemento de autenticación mejorado de VMware ofrece autenticación integrada en Windows y funcionalidad de tarjeta inteligente basada en Windows.

En vSphere 6.5, el complemento de autenticación mejorado de VMware reemplaza al complemento de integración de clientes a partir de vSphere 6.0 y versiones anteriores. El complemento de autenticación mejorado ofrece autenticación integrada en Windows y funcionalidad de tarjeta inteligente basada en Windows. Estas son las únicas dos funciones que se transfirieron del anterior complemento de integración de clientes. El complemento de autenticación mejorado puede funcionar sin problemas si ya tiene el complemento de integración de clientes instalado en el sistema de vSphere 6.0 o una versión anterior. No hay ningún conflicto si ambos complementos están instalados.

Instale el complemento solo una vez solo una vez para habilitar todas las funcionalidades que proporciona.

Nota Cuando habilita los Servicios de federación de Active Directory, el complemento de autenticación mejorado solo se aplica a las configuraciones donde vCenter Server es el proveedor de identidad (Active Directory en LDAP, autenticación integrada de Windows y configuraciones de OpenLDAP).

Procedimiento

1. Abra un explorador web y escriba la URL de vSphere Client.
2. En la parte inferior de la página de inicio de sesión de vSphere Client, haga clic en **Descargar complemento de autenticación mejorado**.
3. Si el navegador bloquea la instalación mediante la emisión de errores de certificado o la ejecución de un bloqueador de elementos emergentes, siga las instrucciones de la Ayuda para solucionar el problema.
4. Guarde el complemento en el equipo y ejecute el archivo ejecutable.
5. Ingrese en el asistente de instalación del complemento de autenticación mejorado de VMware y del servicio de complementos de VMware que se ejecutan en forma sucesiva.
6. Cuando finalicen las instalaciones, actualice el explorador.
7. En el cuadro de diálogo Solicitud de protocolo externo, haga clic en **Iniciar aplicación** para ejecutar el complemento de autenticación mejorado.

   El vínculo para descargar el complemento desaparece de la página de inicio de sesión.

Redireccionar una instancia de vCenter Server a otra instancia de vCenter Server en un dominio diferente

Puede mover una instancia de vCenter Server de un dominio de vSphere a otro. Los servicios como el etiquetado y la concesión de licencias se conservan y se migran a un nuevo dominio.

Se admiten los siguientes casos de uso:

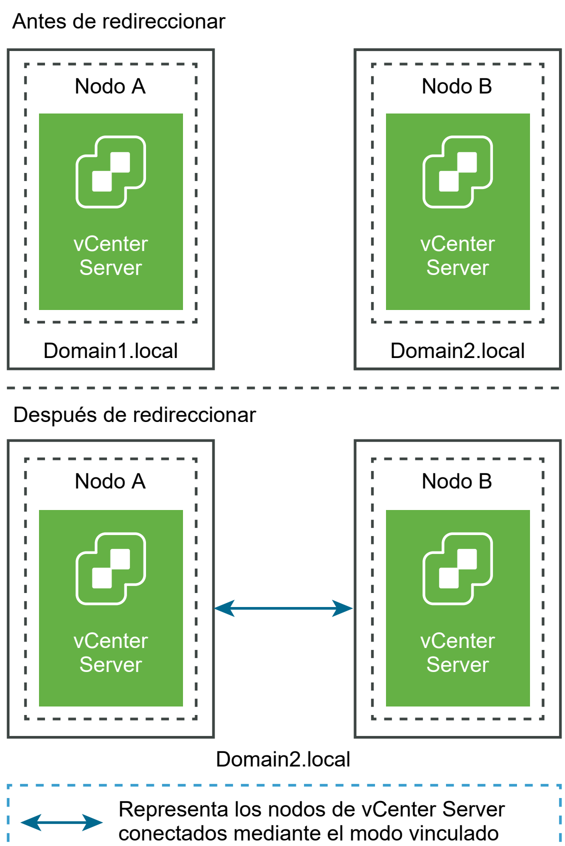
- Puede migrar una instancia de vCenter Server de un dominio existente a otro con replicación o sin ella. La instancia migrada de vCenter Server se mueve de su dominio de Single Sign-On actual y se une al otro dominio existente como otra instancia de vCenter Server conectada mediante Enhanced Linked Mode.
  - Consulte Redireccionar un nodo de vCenter Server único a un dominio existente sin un socio de replicación para obtener instrucciones sobre cómo redireccionar un único nodo integrado de un dominio a un dominio existente sin un partner de replicación.
  - Consulte Redireccionar un nodo de vCenter Server a un dominio existente con un socio de replicación para obtener instrucciones sobre cómo redireccionar un nodo integrado de un dominio a un dominio existente mediante la replicación.
- Puede migrar una instancia de vCenter Server de un dominio existente a un dominio recién creado (en el que la instancia migrada de vCenter Server es la primera instancia). Consulte Redireccionar un nodo de vCenter Server a un dominio nuevo para obtener instrucciones sobre este tipo de redireccionamiento. En este caso, no existe ningún partner de replicación.

Redireccionar un nodo de vCenter Server único a un dominio existente sin un socio de replicación

Puede redireccionar una única instancia de vCenter Server de un dominio de Single Sign-On a un dominio existente de Single Sign-On sin un socio de replicación. Cada dominio de Single Sign-On contiene una única instancia de vCenter Server.

Consulte Figura 5-1. Redireccionar una única instancia de vCenter Server de un dominio a un dominio existente para obtener un ejemplo de redireccionamiento de una única instancia de vCenter Server de un dominio a otro dominio existente. Este es uno de los varios métodos para crear un nodo de Enhanced Linked Mode. En este caso, no hay ninguna replicación.

Figura 5-1. Redireccionar una única instancia de vCenter Server de un dominio a un dominio existente



Requisitos previos

- El redireccionamiento solo se admite en vCenter Server 6.7 Update 1 y versiones posteriores.
- Debe redirigir a un vCenter Server que sea de la misma versión.
- Para impedir una pérdida de datos, cree una copia de seguridad basada en archivo de cada nodo antes de redireccionar vCenter Server.

Procedimiento

1. Asegúrese de que ambos nodos de vCenter Server estén encendidos antes de iniciar el proceso de redireccionamiento.

2. (opcional) Ejecute el comando de modo de comprobación previa. El modo de comprobación previa recopila el etiquetado (etiquetas y categorías) y los datos (funciones y privilegios) de autorización de vCenter Server. La comprobación previa no migra datos, pero busca conflictos entre las instancias de vCenter Server de origen y destino. Por ejemplo, ejecute una comprobación previa con la CLI siguiente:

   ```
   cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
   ```

   Nota La comprobación previa no es necesaria si no existe ningún socio de replicación (se redirecciona a un dominio recién creado).

   Consulte Sintaxis del comando de redireccionamiento del dominio a fin de acceder a las definiciones de argumentos para el comando `cmsso-util domain-repoint`.

   La comprobación previa escribe los conflictos en el directorio `/storage/domain-data`.

3. (opcional) Revise los conflictos y aplique resoluciones para todos los conflictos o una resolución independiente para cada uno.

   Las resoluciones de conflictos son:

   - Copiar: crea una copia duplicada de los datos en el dominio de destino.
   - Omitir: omite copiar los datos en el dominio de destino.
   - Combinar: combina el conflicto sin crear duplicados.

   Nota El modo de resolución predeterminado para los conflictos de Autorización y Etiquetas es Copiar, a menos que se anule en los archivos con conflictos que se generan durante la comprobación previa.

4. Ejecute el comando `execute`. En el modo de ejecución, se leen los datos generados durante el modo de comprobación previa y se importan en el nodo de destino. A continuación, se redirecciona vCenter Server al dominio de destino. Por ejemplo, si desea redireccionar sin un socio de replicación, ejecute el comando `execute` con los siguientes elementos:

   ```
   cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
   ```

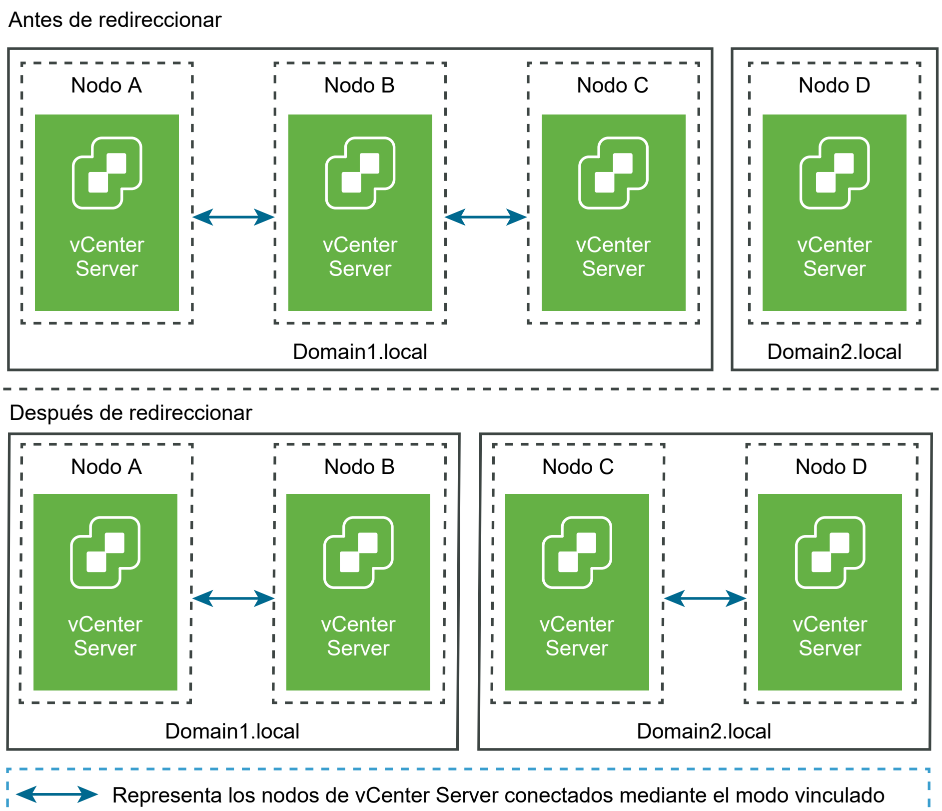
   Consulte Sintaxis del comando de redireccionamiento del dominio a fin de acceder a las definiciones de argumentos para el comando `cmsso-util domain-repoint`.

Redireccionar un nodo de vCenter Server a un dominio existente con un socio de replicación

Puede redireccionar una instancia de vCenter Server de un dominio de Single Sign-On a un dominio existente mediante un partner de replicación.

Consulte Figura 5-2. Redireccionar una instancia de vCenter Server de un dominio a un dominio existente para obtener un ejemplo de redireccionamiento a un dominio existente. En este caso, hay una replicación.

Figura 5-2. Redireccionar una instancia de vCenter Server de un dominio a un dominio existente



Requisitos previos

- El redireccionamiento solo se admite en vCenter Server 6.7 Update 1 y versiones posteriores.
- Debe redirigir a un vCenter Server que sea de la misma versión.
- Para impedir una pérdida de datos, cree una copia de seguridad basada en archivo de cada nodo antes de redireccionar vCenter Server.

Procedimiento

1 Apague el nodo (por ejemplo, el nodo C) que desea redireccionar (mover a un dominio diferente).

2 Retire el nodo de vCenter Server que va a redireccionar. Por ejemplo, para retirar el nodo C, inicie sesión en el nodo B (en el dominio original) y ejecute el siguiente comando:

```
cmsso-util unregister --node-pnid Node_C_FQDN --username
Node_B_sso_administrator@sso_domain.com --passwd Node_B_sso_adminuser_password
```

Después de cancelar el registro del nodo C, se reinician los servicios. Las referencias al nodo C se eliminan del nodo B y de los otros nodos vinculados con el nodo C en el dominio original.

3 Encienda el nodo C para comenzar el proceso de redireccionamiento.

4 (opcional) Ejecute el comando de modo de comprobación previa. El modo de comprobación previa recopila el etiquetado (etiquetas y categorías) y los datos (funciones y privilegios) de autorización de vCenter Server. La comprobación previa no migra datos, pero comprueba los conflictos entre las instancias de vCenter Server de origen y destino. Por ejemplo, ejecute una comprobación previa con la CLI siguiente:

```
cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-
fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --
dest-domain-name destination_PSC_domain
```

Nota La comprobación previa no es necesaria si no existe ningún socio de replicación (se redirecciona a un dominio recién creado).

Consulte Sintaxis del comando de redireccionamiento del dominio a fin de acceder a las definiciones de argumentos para el comando `cmsso-util domain-repoint`.

La comprobación previa escribe los conflictos en el directorio `/storage/domain-data`.

5 (opcional) Compruebe los conflictos y aplique resoluciones para todos los conflictos o una resolución independiente para cada uno.

Las resoluciones de conflictos son:

- Copiar: crea una copia duplicada de los datos en el dominio de destino.
- Omitir: omite copiar los datos en el dominio de destino.
- Combinar: combina el conflicto sin crear duplicados.

Nota El modo de resolución predeterminado para los conflictos de Autorización y Etiquetas es Copiar, a menos que se anule en los archivos con conflictos que se generan durante la comprobación previa.

6 Ejecute el comando execute. En el modo de ejecución, se leen los datos generados durante el modo de comprobación previa y se importan en el nodo de destino. A continuación, se redirecciona vCenter Server al dominio de destino. Por ejemplo, ejecute el comando de ejecución con lo siguiente:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --
replication-partner-fqdn FQDN _of_destination_node --replication-partner-admin
destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

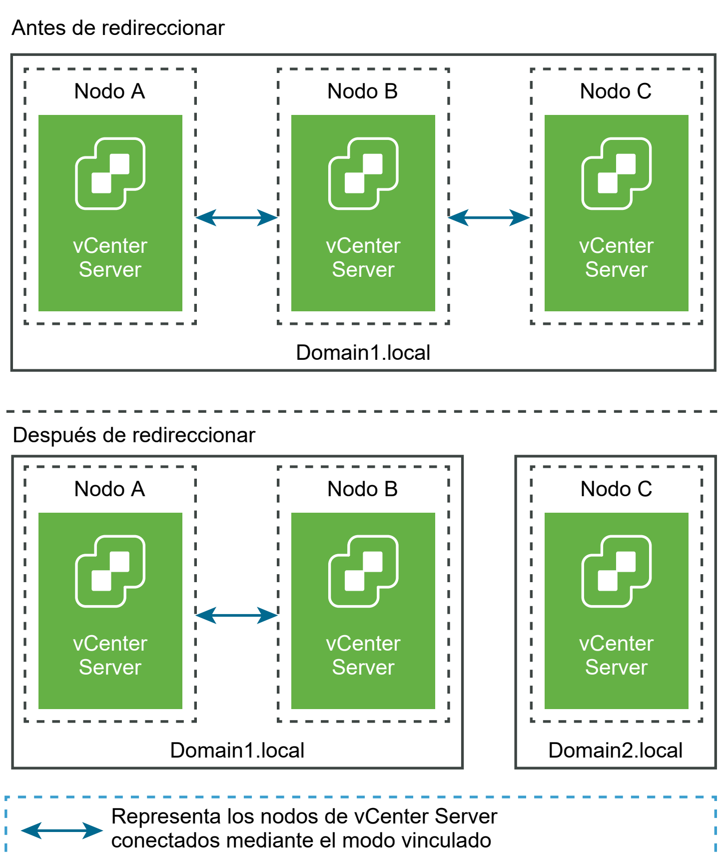
Consulte Sintaxis del comando de redireccionamiento del dominio a fin de acceder a las definiciones de argumentos para el comando `cmsso-util domain-repoint`.

Redireccionar un nodo de vCenter Server a un dominio nuevo

Puede redireccionar una instancia de vCenter Server de un dominio existente a un dominio recién creado.

Consulte Figura 5-3. Redireccionar una instancia de vCenter Server de un dominio a un dominio nuevo para obtener un ejemplo de redireccionamiento a un dominio nuevo. En este caso, no existe ningún socio de replicación.

Figura 5-3. Redireccionar una instancia de vCenter Server de un dominio a un dominio nuevo



Requisitos previos

- El redireccionamiento solo se admite en vCenter Server 6.7 Update 1 y versiones posteriores.
- Debe redirigir a un vCenter Server que sea de la misma versión.
- Para impedir una pérdida de datos, cree una copia de seguridad basada en archivo y una instantánea en estado apagado de cada nodo antes de redireccionar vCenter Server.

Procedimiento

1. Apague el nodo (por ejemplo, el nodo C) que desea redireccionar (mover a un dominio diferente).
2. Retire el nodo de vCenter Server que va a redireccionar. Por ejemplo, para retirar el nodo C, inicie sesión en el nodo B (en el dominio original) y ejecute el siguiente comando:

   ```
   cmsso-util unregister --node-pnid Node_C_FQDN --username
   Node_B_sso_administrator@sso_domain.com --passwd Node_B_sso_adminuser_password
   ```

   Después de cancelar el registro del nodo C, se reinician los servicios. Las referencias al nodo C se eliminan del nodo B y de los otros nodos vinculados con el nodo C en el dominio original.
3. Encienda el nodo C para comenzar el proceso de redireccionamiento.
4. Ejecute el comando execute. En el modo de ejecución, se leen los datos generados durante el modo de comprobación previa y se importan en el nodo de destino. A continuación, se redirecciona vCenter Server al dominio de destino. Por ejemplo, si redirecciona sin un socio de replicación (redireccionamiento a un dominio nuevo), ejecute el comando execute con los siguientes elementos:

   ```
   cmsso-util domain-repoint -m execute --src-emb-admin Administrator  --dest-domain-name
   destination_PSC_domain
   ```

   Consulte Sintaxis del comando de redireccionamiento del dominio a fin de acceder a las definiciones de argumentos para el comando `cmsso-util domain-repoint`.

Sintaxis del comando de redireccionamiento del dominio

Puede usar argumentos de comandos para establecer los parámetros de ejecución del comando de redireccionamiento del dominio.

La CLI `cmsso-util domain-repoint` redirecciona vCenter Server de un dominio a otro.

Puede agregar una lista de argumentos separados por un espacio en el comando de redireccionamiento de la CLI.

Utilice el siguiente comando para redireccionar una instancia de vCenter Server a otro nodo de vCenter Server:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn
FQDN _of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --
dest-domain-name destination_PSC_domain
```

Argumento	Descripción
`-m`, `--mode`	*mode* puede ser `pre-check` o `execute`. El argumento `pre-check` ejecuta el comando en el modo de comprobación previa. El argumento `execute` ejecuta el comando en el modo de ejecución.
`-spa`, `--src-psc-admin`	Nombre de usuario de administrador de SSO para la instancia de origen de vCenter Server. No anexe `@`*domain*.
`-dpf`, `--dest-psc-fqdn`	El FQDN de la instancia vCenter Server que se redirigirá.
`-dpa`, `--dest-psc-admin`	Nombre de usuario de administrador de SSO para la instancia de destino de vCenter Server. No anexe `@`*domain*.
`-ddn`, `--dest-domain-name`	Nombre de dominio SSO de la instancia de destino de vCenter Server.
`-dpr`, `--dest-psc-rhttps`	(Opcional) Puerto HTTPS para la instancia de destino de vCenter Server. Si no está configurada, se usa el valor predeterminado `443`.
`-dvf`, `--dest-vc-fqdn`	El FQDN de la instancia de vCenter Server que redirige a la instancia de destino de vCenter Server. vCenter Server se utiliza para comprobar si hay conflictos de datos de componentes en el modo de comprobación previa. Si no se proporciona, las comprobaciones de conflictos se omiten y se aplica la resolución predeterminada (copiar) para los conflictos hallados durante el proceso de importación. **Nota** Este argumento es opcional si el dominio de destino no tiene una instancia de destino de vCenter Server. Si ya existe una instancia de vCenter Server en el dominio de destino, este argumento es obligatorio.
`-sea`, `--src-emb-admin`	Administrador para vCenter Server con instancia integrada de vCenter Server. No anexe `@domain` al identificador de administrador.
`-rpf`, `--replication-partner-fqdn`	(Opcional) El FQDN del nodo de partner de replicación al que se replica vCenter Server.
`-rpr`, `--replication-partner-rhttps`	(Opcional) El puerto HTTPS para el nodo de replicación. Si no se establece, se usa el valor predeterminado `443`.
`-rpa`, `--replication-partner-admin`	(Opcional) Nombre de usuario del administrador de SSO de la instancia de vCenter Server del partner de replicación.
`-dvr`, `--dest-vc-rhttps`	(Opcional) El puerto HTTPS para la instancia de vCenter Server que apunta a la instancia de destino de vCenter Server. Si no está configurada, se usa el valor predeterminado `443`.
`--ignore-snapshot`	(Opcional) Se pasan por alto las advertencias de la instantánea.

Argumento	Descripción
`--no-check-certs`	(Opcional) Se pasan por alto las validaciones de certificación.
`--debug`	(Opcional) Se recuperan los detalles de ejecución del comando.
`-h`, `--help`	(Opcional) Se muestra el mensaje de ayuda del comando `cmsso-util domain repoint`.

Descripción de los conflictos de etiquetado y autorización

Cuando se ejecuta el comando de redireccionamiento del dominio en el modo de comprobación previa, los datos de vCenter Server se exportan y se examinan, y los conflictos se escriben en un archivo.

Los siguientes datos se exportan a la carpeta `/storage/domain-data/` o `ProgramData/VMWare/vCenterServerdata/domain-data`:

- `All_Privileges.json`
- `All_Roles.json`
- `All_TagCategories.json`
- `All_Tags.json`

Estos archivos contienen todos los datos (autorización y etiquetado) de la instancia de vCenter Server en la que se ejecutó este comando.

Si se proporciona una instancia secundaria de vCenter Server mediante la opción `-dvf` o `--dest-vc-fqdn` , también se exportan los conflictos a la misma carpeta:

- `Conflicts_Roles.json`
- `Conflicts_TagCategories.json`
- `Conflicts_Tags.json`

El siguiente es un archivo de conflictos de ejemplo:

```
<---- Sample Conflict file code block --->
     {
  "global" : {
    "resolution" : "MERGE|SKIP|COPY",
    "description" : "Default resolution option used to resolve Role Conflicts is COPY. The
conflicts list describes the differences between Role entities on source and target vCenter
Server. If
the source information represents an empty JSON array, it simply means that all the entity
attributes from source and target are identical. If the source lists few entries, it means
that only these entity attributes are missing from the target. If the target lists few
entries,
it means that only these entity attributes are missing from the source. Though a global
resolution
can be set, it can also be overridden at each conflict level by providing individual
```

```
resolution
mode."
  },
  "conflicts-count" : 1,
  "conflicts-list" : {
    "NoCryptoAdmin" : {
      "source" : {
        "privileges" : "[]"
      },
      "target" : {
        "privileges" : "[Group-1.SamplePriv-1, Group-1.SamplePriv-4, Group-2.SamplePriv-10,
Group-2.SamplePriv-3, Group-2.SamplePriv-7, Group-3.SamplePriv-2, Group-3.SamplePriv-9]"
      },
      "resolution" : ""
    }
}
<----- End of code block --->
```

Las partes de los archivos de conflicto de ejemplo son las siguientes:

- `description`. Proporciona los detalles sobre cómo se lee y se comprende el archivo de conflictos correspondiente.
- `source` y `target`. Objetos JSON que enumeran solo las diferencias entre los objetos de vCenter Server de origen y de destino.
- `resolution`. El usuario proporciona una resolución válida. Las resoluciones válidas son `MERGE`, `COPY` y `SKIP`.

Para especificar la resolución de conflictos, puede proporcionar una opción predeterminada de resolución de todos los conflictos en la sección `"global": "resolution" = "MERGE|SKIP|COPY"`. Si no proporciona un tipo de resolución global válida para `resolution` o la deja sin editar, el sistema utiliza `COPY` como la opción de resolución predeterminada.

También puede proporcionar una opción de resolución válida para cada uno de los conflictos mediante la edición de la propiedad `resolution` en cada nivel de conflicto que reemplaza a la opción de resolución global.

Los tipos de conflictos que aparecen en Tabla 5-1. Tipos de conflictos.

Tabla 5-1. Tipos de conflictos

Conflicto	Propiedades utilizadas para comparar objetos por categoría	Tipos de conflictos	Propiedades en conflicto	Opciones de resolución de conflictos
Conflicto de función	■ `name`: nombre de la categoría. ■ `privilegeId`: lista de privilegios de la función.	Los conflictos con `RoleName` se producen mientras hay importación de funciones y una función con el mismo nombre en la instancia de destino de vCenter Server, pero con diferentes privilegios.	Las propiedades que pueden estar en conflicto si hay un conflicto de tipo `RoleName` pueden ser `Privileges`.	■ `COPY`. Se crea una copia de la función en conflicto en la instancia de destino de vCenter Server con `--copy` anexado al nombre de la función. La nueva función se crea con un nuevo identificador de función con el mismo conjunto de identificadores de privilegios. En la tabla `VPX_ACCESS`, se actualizó el identificador de la nueva función. El identificador de la nueva función se aplica al conflicto con el nombre de la función y conflicto con el identificador de la función. **Nota** La opción de resolución predeterminada para resolver conflictos con las funciones es `COPY`. ■ `MERGE`. La opción `MERGE` se resuelve en la siguiente secuencia: a Si la instancia de origen de vCenter Server tiene una función con el mismo nombre y la misma lista de privilegios que una función en la instancia de destino de vCenter Server, pero los identificadores de la función son diferentes, se utiliza el identificador de la función de la instancia de destino de vCenter Server y se actualiza en la tabla `VPX_ACCESS`. b Si la instancia de origen de vCenter Server tiene una función con el mismo nombre que una función en la instancia

Tabla 5-1. Tipos de conflictos (continuación)

Conflicto	Propiedades utilizadas para comparar objetos por categoría	Tipos de conflictos	Propiedades en conflicto	Opciones de resolución de conflictos
				de destino de vCenter Server, pero con una lista de privilegios diferentes, entonces las listas de privilegios de ambas funciones se combinan. ■ SKIP. No realice ninguna acción. La función específica se pasa por alto.
Conflicto de categoría de etiqueta: un nombre de categoría debe ser único en una instancia de vCenter Server.	■ name: nombre de la categoría. ■ cardinality: cardinalidad de la categoría, ya sea Única o Múltiples. ■ associableEntityType: lista de objetos de vCenter Server que se pueden asociar con una etiqueta de esta categoría. El valor All indica todos los objetos de vCenter Server.	Puede verse solo un tipo de conflicto al importar categorías de etiquetas: el conflicto CategoryName. Este conflicto indica que ya existe una categoría con el mismo nombre en la instancia de destino de vCenter Server, pero con propiedades diferentes (cardinality o associableEntityType).	Las propiedades que pueden estar en conflicto en el tipo de conflicto CategoryName pueden ser al menos de uno de dos tipos: Cardinality o AssociableTypes.	■ COPY. Se crea una copia de la categoría en conflicto en la instancia de destino de vCenter Server con --copy anexado al nombre de la categoría. La nueva categoría se crea con el mismo nombre de propiedad, como se muestra en la instancia de origen de vCenter Server. Todas las etiquetas que figuraban en esta categoría se importan en la recién creada CategoryCopy. **Nota** La opción de resolución predeterminada para los conflictos de CategoryName es COPY. ■ MERGE. Las propiedades en conflicto se combinan con la categoría que ya está presente en el SSO. Las propiedades se combinan de las siguientes maneras: a Description. Se utiliza la descripción que ya está presente. b Cardinality. La cardinalidad no se puede reducir. Si hay un conflicto de cardinalidad, esta se

Tabla 5-1. Tipos de conflictos (continuación)

Conflicto	Propiedades utilizadas para comparar objetos por categoría	Tipos de conflictos	Propiedades en conflicto	Opciones de resolución de conflictos
				establece en multiple. No se puede reducir al tipo de cardinalidad única. c AssociableTypes. Si los valores de associableEntityType son nulos, se establece como nula. De lo contrario, los tipos Objects se combinan. ■ SKIP. No realice ninguna acción. Todas las etiquetas se importan en la categoría que ya existe.
Conflicto de etiquetas: un objeto tag siempre pertenece a un objeto category. El nombre de una etiqueta debe ser único solo dentro de una categoría.	■ name ■ description	Puede verse solo un tipo de conflicto al importar etiquetas: el conflicto TagName. Este conflicto indica que ya existe una etiqueta con el mismo nombre en la misma categoría y en la instancia de destino de vCenter Server, pero con propiedades diferentes.	Las propiedades que pueden estar en conflicto si hay un conflicto de tipo TagName pueden ser Description.	■ COPY. Se crea una copia de la etiqueta en conflicto en la instancia de destino de vCenter Server con --copy anexado al nombre de la etiqueta. Tome MoRef (identificador de etiqueta interno) de la etiqueta recién creada y actualice la asociación de etiquetas, si es necesario. **Nota** La opción de resolución predeterminada para los conflictos de CategoryName es COPY. ■ MERGE. Mantenga la descripción actual. Tome MoRef (identificador de etiqueta interno) y actualice una o más asociaciones de etiquetas, si es necesario. ■ SKIP. No realice ninguna acción. No cree esta etiqueta. Limpie las asociaciones de etiquetas.

Consideraciones de licencias para redirigir un dominio de vCenter Server

El redireccionamiento de un dominio copia las claves de licencia en un dominio nuevo. Al copiar las claves de licencia, es posible garantizar que se mantengan licencias válidas para todos los activos después del redireccionamiento.

vCenter Server realiza un seguimiento del uso de licencias por dominio. Si se utiliza una clave en más de un dominio, debe asegurarse de que el uso agregado de la clave no supere su capacidad. Para simplificar la administración de licencias, elimine cada licencia copiada en un segundo dominio y asigne una nueva licencia a los activos.

Tenga en cuenta los siguientes dos casos:

- Claves de licencia que ya no se usan (es decir, se asignaron a activos) en el dominio original tras el redireccionamiento.
- Claves de licencia que se encuentran en uso (es decir, se asignaron a activos) en varios dominios.

Claves de licencia no en uso en un dominio

Si después de completar el redireccionamiento, una clave de licencia se muestra en más de un dominio, pero no se encuentra en uso en algunos de esos dominios, puede eliminar la clave de licencia de cualquier dominio en el que no se use. Consulte “Quitar licencias” en *Administrar vCenter Server y hosts* para obtener instrucciones sobre la forma de eliminar las licencias en vCenter Server.

Claves de licencia en uso en varios dominios

Si después de completar el redireccionamiento, una clave de licencia se encuentra en uso (es decir, se asignó a activos) en más de un dominio, antes de eliminar la clave de licencia de todos menos un dominio, primero se debe asignar una clave de licencia diferente a cada activo en los dominios de los que se eliminará la clave de licencia. Dos enfoques comunes:

- Si dispone de otras claves de licencia con suficiente capacidad sin utilizar, puede usar esas claves en lugar de una clave de licencia que planee eliminar. Consulte “Asignar una licencia a varios activos” en *Administrar vCenter Server y hosts* para asignar licencias en vCenter Server.
- Puede dividir las claves de licencia que se utilizan en más de un dominio en claves de licencia independientes, una para cada dominio. Para dividir las claves de licencia, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2006972. Para determinar la capacidad que se debe incluir en cada una de las claves de licencia en las que se dividirá la original, consulte “Ver información de licencias” en *Administrar vCenter Server y hosts* para ver el uso de la clave de licencia en vCenter Server para cada uno de los dominios.

A continuación, es posible agregar cada una de las claves de licencia resultantes a un dominio diferente y asignarlas en vCenter Server a los activos con licencia de la clave de licencia original. Consulte “Crear nuevas licencias” en *Administrar vCenter Server y hosts* para crear licencias y “Asignar una licencia a varios activos” en *Administrar vCenter Server y hosts* para asignar una licencia a varios activos.

Después de que se asignan diferentes licencias a todos los activos, la clave de licencia original, que ya no es válida, se puede eliminar de todos los dominios mediante vCenter Server. Consulte “Quitar licencias” *Administrar vCenter Server y hosts*.

Solucionar problemas de instalación o implementación de vCenter Server

6

Los temas de solución de problemas de implementación de vCenter Server proporcionan soluciones a problemas que podrían surgir durante el proceso de implementación de vCenter Server Appliance.

Este capítulo incluye los siguientes temas:

- Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server

Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server

Puede recopilar archivos de registro de instalación o actualización de vCenter Server. Si se produce un error en una instalación o actualización, la comprobación de los archivos de registro puede ayudar a identificar el origen del error.

También puede recopilar archivos de registro de implementación de vCenter Server.

- Recuperar registros de instalación de forma manual

  Puede recuperar manualmente los archivos de registro de instalación para examinarlos.

- Recopilar archivos de registro de implementación para vCenter Server Appliance

  Si se produce un error en la implementación de vCenter Server Appliance, puede recuperar y analizar los archivos de registro para determinar el motivo del error.

- Exportar un paquete de soporte de vCenter Server para solución de problemas

  Puede exportar el paquete de soporte de la instancia de vCenter Server en el dispositivo para solucionar problemas mediante la dirección URL que aparece en la pantalla de inicio de la DCUI.

Recuperar registros de instalación de forma manual

Puede recuperar manualmente los archivos de registro de instalación para examinarlos.

Procedimiento

1 Desplácese hasta las ubicaciones de los archivos de registro de instalación.

- El directorio `%PROGRAMDATA%\VMware\vCenterServer\logs`, generalmente `C:\ProgramData\VMware\vCenterServer\logs`
- El directorio `%TEMP%`, generalmente `C:\Users\`*`username`*`\AppData\Local\Temp`

Los archivos en el directorio `%TEMP%` incluyen `vc-install.txt`, `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log` y `vim-vcs-msi.log`.

2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Recopilar archivos de registro de implementación para vCenter Server Appliance

Si se produce un error en la implementación de vCenter Server Appliance, puede recuperar y analizar los archivos de registro para determinar el motivo del error.

La ruta de acceso completa a los archivos de registro aparece en el asistente de implementación de vCenter Server Appliance.

En caso de error en el primer arranque, puede descargar el paquete de soporte en un equipo host Windows y revisar los archivos de registro para determinar qué script de primera opción de arranque produjo el error. Consulte Exportar un paquete de soporte de vCenter Server para solución de problemas.

Procedimiento

1 En la máquina Windows que utiliza para implementar vCenter Server Appliance, desplácese hasta la carpeta de los archivos de registro.

Si inició sesión como administrador, la carpeta predeterminada es `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller`.

2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Exportar un paquete de soporte de vCenter Server para solución de problemas

Puede exportar el paquete de soporte de la instancia de vCenter Server en el dispositivo para solucionar problemas mediante la dirección URL que aparece en la pantalla de inicio de la DCUI.

También puede recopilar el paquete de soporte del shell de Bash de vCenter Server Appliance mediante la ejecución del script `vc-support.sh`.

El paquete de soporte se exporta en formato `.tgz`.

Procedimiento

1 Inicie sesión en el equipo host de Windows en el que desea descargar el paquete.

2 Abra un explorador web y escriba la URL del paquete de soporte que se muestra en la DCUI.

https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3 Escriba el nombre de usuario y la contraseña del usuario raíz.

4 Haga clic en **Entrar**.

El paquete de soporte se descarga como archivo `.tgz` en su equipo Windows.

5 (opcional) Para determinar cuál fue el script de primer arranque que generó un error, examine el archivo `firstbootStatus.json`.

Si ejecutó el script `vc-support.sh` en el shell de Bash de vCenter Server Appliance, para examinar el archivo `firstbootStatus.json`, ejecute

```
cat /var/log/firstboot/firstbootStatus.json
```